HELSINGIN KAUPPAKORKEAKOULU
Laskentatoimen ja rahoituksen laitos

SÄHKÖISTEN SOPIMUSTEN TEKEMINEN VERKOSSA SUOMESSA

Yritysjuridiikka
Pro Gradu –tutkielma
Henrik Luoto (k72506)
Kevät 2008

Laskentatoimen ja rahoituksen laitoksen laitosneuvoston kokouksessa 13/5 2008

hyväksytty arvosanalla erinomainen, 90p.

Tarkastajat:

OTT, Matti Rudanko

KTM, Mikko Viemerö

HELSINGIN KAUPPAKORKEAKOULU – LASKENTATOIMEN JA RAHOITUKSEN LAITOS

Yritysjuridiikka

Tekijä
Henrik Luoto

Työn nimi
Sähköisten sopimusten tekeminen verkossa Suomessa

Työn laji	**Aika**	**Sivumäärä**
Pro Gradu –tutkielma	Huhtikuu 2008	IV+87

Tiivistelmä

Tutkielman tarkoituksena on antaa lukijalleen kokonaisvaltainen kuva sähköisten sopimusten tekemiseen verkossa liittyvistä oikeudellisista kysymyksistä Suomessa. Tutkielmassa käydään läpi sähköisten sopimusten syntymiseen, luonteeseen, poikkeuksiin, rajoitteisiin, epävarmuustekijöihin sekä muihin erityiskysymyksiin liittyviä oikeudellisia kysymyksiä. Tutkielmassa keskitytään sähköisiin sopimuksiin, jotka edellyttävät vähintäänkin toisen osapuolen aktiivista osallistumista sopimuksen syntymiseen. Käytännössä sähköisiä sopimuksia koskeva kansallinen oikeusnormisto pohjautuu lähes puhtaasti EU-direktiiveihin, joten direktiivien painoarvo tutkielman oikeuslähteinä on merkittävä. Tutkielman ulkopuolelle on rajattu tietokoneiden väliset EDI-sopimukset ja rahoituspalveluiden etäsopimukset.

Uudenlainen toimintaympäristö, jossa fyysisiä tai kulttuurillisia rajoitteita ei perinteisessä mielessä ole, on luonut uusia oikeudellisia kysymyksenasetteluja. Sähköisen sopimisen ja kaupan oikeudellisen sääntelyn perusedellytyksenä voidaan pitää oikeusvarmuuden lisäämistä kaikilla lainsäädännön tasoilla. Yleisesti ottaen sopimusoikeuden normit soveltuvat sähköisiin sopimuksiin riippumatta sopimuksen muodosta, mahdollistaen lähes kaikki sopimusoikeudelliset kysymyksenasettelut. Kansallisella ja yhteisötasolla toimittaessa sähköisten sopimusten oikeusvarmuus suomalaisen kuluttajan tai elinkeinonharjoittajan näkökulmasta on varsin hyvä mutta maailmanlaajuisella tasolla voidaan sähköisten sopimusten oikeudellisen sääntelyn ja luottamuskysymysten katsoa olevan edelleen varsin sekavassa tilassa. Ongelmaksi on muodostunut epätietoisuus ja tulkinnanvaraisuus sovellettavasta lainsäädännöstä, elinkeinoharjoittajan sijaintipaikasta sekä riitatilanteessa toimivaltaisen tuomioistuimen löytämisestä. Myös käytännön kokemusten, luottamuksen ja käyttäytymismallien puuttumista voidaan pitää esteenä sähköisten sopimusten tekemisen yleistymiselle ja kasvulle.

Esteitä on pyritty poistamaan kehittämällä osapuolten tunnistamiseen ja sisällön varmistamiseen erilaisia menetelmiä, kuten esimerkiksi kehittyneitä sähköisiä allekirjoituksia. Tekijän tunnistaminen ja sisällön varmentaminen edellyttävät erityisjärjestelyjä tietoverkoissa, kuten etukäteen sovittuja menettelytapoja osapuolten välillä tai riittävät vaatimukset täyttävän sähköisen allekirjoituksen käyttämistä. Kehittyneet sähköiset allekirjoitukset ovat kuitenkin yleistyneet paljon hitaammin kuin vuosituhanteen vaihteessa oletettiin. Hitaaseen kehitykseen ei löydy yksiselitteistä syytä. Kehityksen Tähän ovat vaikuttaneet muun muassa oikeusvarmuuden, luottamuksen ja kattavan oikeuskäytännön puute, tekniikan monimutkaisuus, alikehittyneet markkinat sekä tarjottavien palveluiden suppea lukumäärä.

Tulevaisuudessa kynnys sähköisten sopimusten solmimiselle laskee entisestään sähköisten varmenteiden levitessä erilaisille älykorttialustoille, kuten esimerkiksi pankkikorteille ja matkapuhelinoperaattoreiden SIM-korteille. Myös tietoyhteiskunnan palvelujen kehittämisen yhteydessä on hahmoteltu esimerkiksi sormenjälkeen perustuvaa biometrisen laatuvarmenteen kehittämisestä.

Avainsanat
Sähköinen sopimus, sähköisten sopimusten syntyminen, sähköinen allekirjoitus, direktiivi sähköisestä kaupasta, direktiivi sähköisiä allekirjoituksia koskevista yhteisön puitteista, sähköisen sopimuksen muotovaatimukset, sähköisen sopimuksen todentaminen, vakioehdot sähköisessä sopimuksessa

Sisällysluettelo

Kuvat

Kuviot

Taulukot

Lyhenteet

CEN	Comité Européen de Normalisation
CISG	United Nations Convention on Contracts for the International Sale of Goods
CWA	CEN Workshop Agreement
EDI	Electronic Data Interchange, katso lyhenne OVT
EU	Euroopan unioni
EY	Euroopan yhteisöt
GUIDEC	General Usage for International Digitally Ensured Commerce
HE	Hallituksen esitys
HST	Henkilön sähköinen tunnistaminen
ICC	International Chambre of Commerce, Kansainvälinen kauppakamari
IP	Internet Protocol
IPSec	Internet Protocol Security Architecture
KSL	Kuluttajansuojalaki (38/1978)
OECD	Organization for Economic Cooperation and Development
OikTL	Laki varallisuusoikeudellisista oikeustoimista
OVT	Organisaatioiden välinen tiedonsiirto
PKI	Public Key Infrastructure, julkisen salakirjoitusavaimen järjestelmä
SSCD	Secure Signature Creation Device
SSL	Secure Sockets Layer
TietoyhtPalvL	Laki tietoyhteiskunnan palvelujen tarjoamisesta (1607/1993)
TUPAS	Tunnistuspalvelu asiointipalveluntuottajille
UNCITRAL	United Nations Commission on International Trade Law, YK:n kauppalakikomitea
VM	Valtiovarainministeriö

1. Johdanto

1.1 Taustaa

Sopimusten tekeminen sähköisessä muodossa on yleistynyt vasta viimeisten kymmenen vuoden aikana, vaikka tietoverkot eri muodoissaan ovat olleet murrosvaiheessa jo 1980-luvulta lähtien. Informaatioteknologian nopea kehitys ja sen sovellusten – www-sivujen ja sähköpostin – hyödyntäminen ovat luoneet otollisen ympäristön sopimusten solmimiselle tietoverkoissa. Tietoverkot ovat mahdollistaneet arkisten oikeustoimien, kuten esimerkiksi pankkipalveluiden ja valtionhallinnon palveluiden tekemisen sähköisesti.

Maantieteellisten ja valtiollisten rajoitteiden poistuessa kuluttajille ja elinkeinonharjoittajille on avautunut ennennäkemättömät mahdollisuudet käydä kansainvälistä kauppaa ja tehdä sopimuksia sähköisesti. Ostajat voivat hankkia tavaroita ja palveluita kilpailukykyiseen hintaan vaivattomasti ja toisaalta elinkeinonharjoittajat voivat markkinoida tuotteita maailmanlaajuisesti pienillä taloudellisilla panoksilla.

Sähköisten sopimusten erikoislaatuinen toimintaympäristö on kuitenkin muodostanut sopimusoikeuteen uusia oikeudellisia asetelmia ja kysymyksiä maailmanlaajuisella, yhteisöllisellä ja kotimaisella tasolla. Uudet oikeudelliset kysymyksenasettelut johtuvat verkkokaupan maailmanlaajuisesta ulottuvuudesta sekä nopeasti muuttuvasta toimintaympäristöstä.

Tavanomaisen kaupankäynnin sääntelynormisto kehittyneissä maissa on kattavaa ja yleensä sovellettavissa suoraan sähköiseen kauppaan. Oikeusjärjestelmän pitäisi kuitenkin toimia myös sähköisessä ympäristössä sellaisella varmuudella, ettei väärinkäytöksiä pääse syntymään. Sähköisen sopimisen ja kaupan oikeudellisen sääntelyn perusedellytyksenä voidaan pitää oikeusvarmuuden lisäämistä kaikilla lainsäädännön tasoilla.

1.2 Tutkielmakysymykset ja rajaukset

Tämän tutkielman tarkoituksena on antaa yleiskuva sähköisten sopimusten tekemisestä tietoverkoissa. Tutkielmassa käydään läpi sähköisten sopimusten syntymiseen, luonteeseen, poikkeuksiin, rajoitteisiin, epävarmuustekijöihin sekä muihin erityiskysymyksiin liittyviä oikeudellisia kysymyksiä. Tutkielman ulkopuolelle rajataan tietyt erityistapaukset kuten rahoituspalveluiden etämyyntiin liittyvät sähköiset sopimukset.

Tutkielmassa keskitytään sähköisiin sopimuksiin, jotka vaativat vähintäänkin toisen osapuolen aktiivista osallistumista. Tässä tutkielmassa ei käsitellä tietokoneiden välisiä automatisoituja sopimuksia tai niihin liittyviä tiedonsiirtosopimuksia, kuten esimerkiksi EDI-sopimuksia vaan keskitytään sähköisten sopimusten muihin kategorioihin. EDI-sopimukset rajataan tutkielman ulkopuolelle koska niiden kohdalla sopimusprosessi poikkeaa melko paljon totutusta sopimusoikeudesta ja sisältää erityisen paljon spesifejä tietotekniikkakysymyksiä. Tutkielman ulkopuolelle rajataan myös sähköisessä ympäristössä tehtävät palveluita koskevat käyttäjäehtosopimukset ja ohjelmistoja koskevat lisenssisopimukset omien erikoispiirteittensä vuoksi.

Tutkielmassa käsitellään kuluttajien ja yritysten välisiä sähköisiä sopimuksia niiden käytön laaja-alaisen yleistymisen vuoksi. Yritysten välisiä sähköisiä sopimuksia käsitellään suppeammin johtuen kyseisissä sopimussuhteissa vallitsevasta sopimusvapaudesta sekä niiden tapauskohtaisesta luonteesta.

Tutkielmassa keskitytään sähköisten sopimusten tekemiseen Suomessa, joten Suomen lainsäädännöllä ja erityisesti EU-oikeudella on suuri painoarvo tutkielman oikeuslähteinä. Kansainvälisiä näkökohtia tuodaan lähinnä esille suomalaisen kuluttajan kuluttajansuojaa koskevissa kansainvälisissä kysymyksissä sekä sähköisiä sopimuksia koskevissa erityiskysymyksissä.

Monet sähköisen sopimuksen ongelmakysymykset ilmenevät myös muissa sopimuksentekotilanteissa, mutta tässä tutkielmassa syvennytään erityisesti sähköisen sopimuksen tekemiseen liittyviin spesifeihin piirteisiin ja ongelmakohtiin sekä niiden

ratkaisumalleihin. Teknisiä näkökulmia joudutaan tuomaan esille sopimusten teknisen luonteen ja erikoislaatuisen toimintaympäristön vuoksi.

1.3 Tutkielman rakenne

Tutkielman toisessa luvussa käydään läpi sähköinen sopimus käsitteenä. Sähköisiä sopimuksia koskevaa lainsäädäntöä lähestytään aloittaen maailmanlaajuisesta oikeusnormistosta, siirtyen EY:n lainsäädäntöön ja lopuksi päätyen Suomen kansalliseen lainsäädäntöön. Luvussa keskitytään erityisesti EU-direktiivien käsittelyyn johtuen Euroopan yhteisön oikeuden etusijasta kansalliseen oikeuteen nähden.

Kolmannessa luvussa käsitellään sähköisen sopimuksen syntymisen erityispiirteitä jaottelemalla ne kolmeen eri kategoriaan sekä sitovuusperusteita tarkastelemalla tarjous–vastaus -mekanismin soveltuvuutta sähköisiin sopimuksiin, etäsopimusten luonnetta ja kuluttajansuojaa sekä yritysten välisiä sähköisiä sopimuksia.

Neljännessä luvussa käsitellään sähköisten allekirjoitusten eri kategorioita, joita käytetään sähköisissä ympäristöissä sopimuksien hyväksymiseen. Sähköisten allekirjoitusten eri kategorioiden oikeusvaikutuksiin ja käytön turvallisuuteen kiinnitetään huomiota. Luvussa tuodaan erityisesti esille varmennettu sähköinen allekirjoitus, jonka oikeusvarmuus on rinnastettu yhteisötason lainsäädännössä perinteiseen allekirjoitukseen. Luvussa käsitellään myös sähköisten allekirjoitusten nykytilaa ja tulevaisuudennäkymiä.

Tutkielman viidennessä luvussa käydään läpi sähköisen asiakirjan todentamiseen liittyviä kysymyksiä. Sähköisen asiakirjan todentamisvaatimuksia vertaillaan vastaavanlaisen paperiasiakirjan vaatimuksiin ja erityisesti huomiota kiinnitetään tiedon alkuperän todentamisen, tiedon eheyden ja kiistämättömyyden vaatimuksiin.

Kuudennessa luvussa käsitellään sähköisen sopimuksen muotovaatimuksia. Luvussa käsitellään muotovapaat ja muotovaatimukselliset sähköiset sopimukset sekä niitä koskevat poikkeukset ja rajoitteet.

Seitsemänteen lukuun on koottu sähköisiä sopimuksia koskettavia erityiskysymyksiä. Käsiteltävinä erityiskysymyksinä ovat tekniset ongelmat sähköisiä sopimuksia solmittaessa, kansainväliset sähköiset sopimukset ja niihin sovellettava lainsäädäntö, vakioehdot sähköisissä sopimuksissa, tietoturvallisuus ja yksityisyydensuoja sähköisessä kaupankäynnissä sekä sähköisen kaupankäynnin riskit.

Kahdeksannessa eli viimeisessä luvussa käydään tutkielman sisältöä läpi johtopäätöksiä tehden, silmälläpitäen sähköisten sopimusten tulevaisuudenkehitysnäkymiä.

1.4 Määritelmiä

Tietoyhteiskunnan palvelulla eli *etäpalvelulla* tarkoitetaan tässä tutkielmassa sähköisessä muodossa palvelun vastaanottajan henkilökohtaisesta pyynnöstä toimitettavia palveluita, joista tavallisesti maksetaan korvaus. Tyypillisiä tietoyhteiskunnan palveluja ovat sähköiset palvelut kuten tietokoneohjelmat, viihdepalvelut, verkkokauppa ja siihen liittyvä markkinointi sekä sähköinen asiointi viranomaisten ja pankkien kanssa.[1]

Laatuvarmenteella tarkoitetaan varmennetta, joka täyttää direktiivissä sähköisiä allekirjoituksia koskevista yhteisön puitteista (99/93/EY) säädetyt vaatimukset. Varmenteen tulee olla myöntänyt direktiivin vaatimukset täyttävä laatuvarmenteiden tarjoaja.

Sähköisellä allekirjoituksella tarkoitetaan varmennettua sähköistä allekirjoitusta, joka on määritelty direktiivissä sähköisiä allekirjoituksia koskevista yhteisön puitteista (99/93/EY). Tutkielmassa Sähköisiä allekirjoituksia -luvun alussa sähköisellä allekirjoituksella viitataan kuitenkin sähköiseen allekirjoitukseen laajassa mielessä.

---

[1] KOM 1998/586/EY lopullinen s. 15 ja Laine (toim.) 2001 s. 9.

Sähköisen allekirjoituksen luomisvälineellä tarkoitetaan tehtävään tarvittavan fyysisen laitteen ja sen toiminnan mahdollistavien ohjelmisto- sekä laitteistokomponenttien muodostamaa kokonaisuutta.[2]

Tietoverkolla tarkoitetaan julkista verkkoa, kuten esimerkiksi Internetiä. Toiston välttämiseksi tutkielmassa käytetään myös sanaa verkko synonyyminä sanalle tietoverkko.

Älykortti voi olla muistia sisältävä muistikortti tai prosessorikortti, joka voi sisältää muistin lisäksi erilaisia sovelluksia. Sirukortti toimii vain erityisen lukulaitteen yhteydessä. Pelkän mikropiirin sisältäviä kortteja voidaan käyttää SIM-kortteina matkapuhelimissa. Kortin käyttö vaihtelee siihen ohjelmoitujen toimintojen mukaan. Sähköinen allekirjoitus edellyttää salausprosessorin sisältävää sirukorttia. Alan kirjallisuudessa käytetään usein synonyymejä toimikortti ja smart card.[3] Johdonmukaisuuden ja selkeyden vuoksi tutkielmassa käytetään älykortti-sanaa.

---

[2] Liikenne- ja viestintäministeriö 2005a s. 8.
[3] Järvinen 2003 s. 173–175.

2. Sähköisten sopimusten oikeudellinen sääntely

Sähköiset sopimukset ovat verkkosopimuksia, joissa ei ole mahdollista käyttää perinteistä kirjallista muotoa tai omakätistä allekirjoitusta. Verkkosopimuksille on siis ominaista se, että tahdonilmaisujen vaihto tapahtuu tietoverkon välityksellä. Oikeustoimien tekeminen luotettavasti sähköisesti edellyttää, että niiden tekijä voidaan tunnistaa ja oikeustoimen sisältö pätevästi varmistaa. Jos oikeustoimi on tehty kirjallisesti ja allekirjoitettu omakätisesti, on sen tekijän luotettava tunnistaminen ja oikeustoimen sisällön varmentaminen yleensä mahdollista.[4]

Tietoverkoissa tehtävien oikeustoimien osalta kyseisten vaatimusten täyttyminen ei ole kuitenkaan itsestään selvää. Tekijän tunnistaminen ja sisällön varmentaminen edellyttävät erityisjärjestelyjä tietoverkoissa, kuten etukäteen sovittuja menettelytapoja osapuolten välillä tai riittävät vaatimukset täyttävän sähköisen allekirjoituksen käyttämistä.

Sähköisen sopimuksen tekeminen tietoverkossa on yksi sopimustyyppi muiden joukossa. Sopimusoikeuslainsäädäntöä voidaan yhtälailla soveltaa muiden sopimustyyppien ohella sähköisiin sopimuksiin. Perinteisessä sopimusoikeudessa sähköisiin sopimuksiin liittyviä erityisongelmia ei kuitenkaan ole huomioitu. Uudenlainen toimintaympäristö on luonut tarpeen uudistaa voimassa olevaa lainsäädäntöä sähköisten sopimusten vaatimuksia vastaavaksi.[5]

2.1 Maailmanlaajuinen sääntely

Lähes kaikki sähköisen kaupankäynnin edellytysten luomiseen panostaneet valtiot ovat laatineet sähköistä allekirjoitusta koskevaa lainsäädäntöä. Myös kansainväliset järjestöt ovat panostaneet sähköisten allekirjoitusten kehittämiseen ja standardoimiseen luomalla mallilakeja ja ohjeistusta. Sähköisiä allekirjoituksia koskeva lainsäädäntö ei ole

---

[4] Laine (toim.) 2001 s. 195–197.
[5] Laine (toim.) 2001 s. 2–3.

kuitenkaan maailmanlaajuisesti saanut yhtenäistä asua, mutta kansainvälisen lainharmonisointityön tuloksena ristiriitaisten kansallisten lainsäädösten määrä on vähentynyt.[6] Maailmanlaajuisella sääntelyllä pyritään löytämään ratkaisuja muun muassa tekijänoikeuskysymyksiin, standardeihin, tietoturva-asioihin sekä sähköisiin maksuvälineisiin liittyviin kysymyksiin. Valtioiden verotukselliset ja tietoverkkorikollisuuteen liittyvät näkökulmat ovat myös usein esillä.[7]

Kansainvälisten järjestöjen sähköisiä allekirjoituksia koskevista hankkeista tärkeimpinä voidaan pitää Yhdistyneiden Kansakuntien (YK) kansainvälisen kaupan komission (UNCITRAL[8]) vuonna 2005 laatimaa yleissopimusta[9] *United Nations Convention on the Use of Electronic Communications in International Contracts* ja tätä sopimusta edeltänyttä vuodelta 1996 olevaa UNCITRAL:in sähköisen kaupankäynnin mallilakia.[10]

UNCITRAL:in yleissopimus käsittelee yksinomaan tiettyjä sähköisen sopimustoiminnan erityispiirteitä rakentaen eräänlaisen sääntökerrostuman sopimusoikeuden muiden normien päälle.[11] Yleissopimuksen perustavoitteena on sähköisen muodon syrjimättömyyden takaaminen ja muiden kansainvälisten säännösten päivittäminen sähköisen kaupankäynnin aikakaudelle.[12] Monien maiden nykyiset sähköistä kaupankäyntiä sääntelevät lait pohjautuvat UNCITRAL:in vuoden 1996 mallilakiin.[13]

---

[6] Railas 2005 s. 1279 ja 1290.
[7] Laine 1998 s. 10.
[8] The United Nations Commission on International Trade Law.
[9] Ks http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf. Tätä sopimusta edelsi UNCITRAL:in sekä vuonna 2001 että 1996 tekemät mallilait sähköisistä allekirjoituksista.
[10] Railas 2005 s. 1268. Katso myös Laine 1998 s. 10 ja Laine (toim.) 2001 s. 3–4. Muina tärkeinä aikaisempina hankkeina voidaan pitää kansainvälisen kauppakamarin (ICC) GUIDEC 1997 (General Usage for International Digitally Ensured Commerce) ja WIPO:n (World Intellectual Property Organization) joulukuussa 1996 järjestämää diplomaattista konferenssia tekijänoikeuskonventioiden digitaaliaikaan päivittämisestä.
[11] Railas 2005 s. 1273.
[12] Railas 2005 s. 1275 ja 1290.
[13] Railas 2005 s. 1269.

UNCITRAL:in yleissopimus ja EY:n sähköisiä sopimuksia koskeva lainsäädäntö sisältävät myös osittain yhteneviä säännöksiä sähköisistä sopimuksista ja ehkä tulevaisuudessa onkin mahdollista, että osia UNCITRAL:in yleissopimuksesta harmonisoidaan osaksi EU:n lainsäädäntöä.[14] On kuitenkin selvää, että UNCITRAL:in yleissopimus ja EU:n sähköisen kaupan direktiivi palvelevat eri tarkoituksia. Sähköisen kaupan direktiivissä on omaksuttu sisämarkkinoihin perustuva lähestymistapa ja alkuperämaan periaate, jotka eivät sovellu kansainvälisiin mallilakeihin joiden perustana on oikeudellisen yhdentymisen riittävä taso.[15]

Myös kansainvälinen elinkeinoelämä on harjoittanut itsesäätelyä mm. markkinoinnin, mainonnan, sopimusehtojen ja riitojen ratkaisumekanismien osalta. Kansainvälisen kauppakamarin (ICC[16]) tietoturvallisuusryhmän asiakirja GUIDEC 1997 (General Usage for International Digitally Ensured Commerce) asettaa suuntaviivoja elinkeinoelämän normistojen ja riitojen ratkaisuun. Elinkeinoelämän keskinäinen itsesäätely voi olla toimiva ratkaisu kun osapuolet ovat voimasuhteiltaan tasavahvoja ja voivat osallistua tasapuolisesti sääntöjen luomiseen.[17]

2.2 Yhteisötason sääntely

EY:n sähköisiin sopimuksiin liittyvät oikeuspoliittiset tavoitteet esitettiin ensimmäistä kertaa komission tiedonannossa *Eurooppalaisen elektronisen kaupankäynnin aloite* (KOM 97(157)) vuonna 1977. Aloitteen keskeinen viesti oli sähköisen kaupan voimakkaan kasvun rohkaiseminen. Tiedonannossa asetettiin tulevaisuuden tavoitteiksi pääsy verkkokaupan tuotteisiin ja palveluihin laajasti ja kustannuksiltaan edullisesti,

---

[14] Railas 2005 s. 1290–1291 ja 1276-.
[15] KOM 1998/586/EY lopullinen s. 17. Ks. myös Railas 2005 s. 1290-1291. Yleissopimus päivittää hyödyllisellä tavalla kansainvälisten yleissopimusten määräyksiä sähköisen kaupan aikakaudelle. Jotta pohjoismaat voisivat hyväksyä sopimuksen, tulisi pohjoismaiden luopua United Nations Convention on Contracts for the International Sale of Goods (CISG) konvention osaa II koskevasta varaumasta ja ryhtyä soveltamaan konvention osaa II kansainvälisiin irtaimen kaupan sopimuksiin oikeustoimilain asemasta.
[16] International Chambre of Commerce.
[17] Laine 1998 s. 16.

suotuisan liiketoimintaympäristön edistäminen ja vakaan sekä ennustettavan oikeudellisen kehyksen aikaansaaminen.[18]

EY:n perustamissopimuksen määräykset tavaroiden, palveluiden ja pääomien vapaasta liikkuvuudesta sisämarkkinoilla sekä sijoittautumisoikeudesta soveltuvat myös sähköiseen kauppaan. Perustamissopimuksen säännöksiä yksistään ei ole kuitenkaan pidetty riittävinä turvaamaan sähköisen kaupankäynnin edellytyksiä, minkä vuoksi EU:ssa on luotu joukko sähköistä kaupankäyntiä käsitteleviä direktiivejä.[19]

Nykyään keskeisimpiä sähköisiä sopimuksia sääntteleviä EU-direktiivejä ovat direktiivi sähköisiä allekirjoituksia koskevista yhteisön puitteista (99/93/EY), direktiivi sähköisestä kaupasta (2000/31/EY), direktiivi teknisiä standardeja ja määräyksiä ja tietoyhteiskunnan palveluja koskevia määräyksiä koskevien tietojen toimittamisessa noudatettavasta menettelystä (98/48/EY) sekä direktiivi kuluttajansuojasta etäsopimuksissa (97/7/EY).

2.2.1 Direktiivi sähköisestä kaupasta

Sähköisen kaupankäynnin direktiivillä eli sähköisen kaupankäynnin kehysdirektiivillä on varmistettu, että tietoyhteiskunnan palveluiden käyttäjät ja tuottajat voivat saada täyden hyödyn EU:ssa sisämarkkinoista, palveluiden tarjoamisen vapaudesta sekä sijoittautumisvapaudesta ilman lainsäädännöllisiä rajoja.[20] Direktiivi on erityisen merkittävä sähköisen kaupankäynnin osalta sen sisältämien periaatteellisten linjavetojen vuoksi.

Direktiivissä pyritään puuttumaan vain sisämarkkinoiden kannalta ehdottoman välttämättömiin seikkoihin, jotta törmäyksiltä kansallisten oikeusjärjestelmien kanssa vältytään. Sen oikeudelliset puitteet on pyritty luomaan kevyiksi, kehittyviksi ja joustaviksi.[21] Direktiivin tarkoituksena on edistää markkinaosapuolten roolia ja

---

[18] Laine (toim.) 2001 s. 6.
[19] Laine (toim.) 2001 s. 6.
[20] SEK/2000/0386 lopullinen ks. kohta 2. Direktiivin tarkoitus.
[21] KOM 1998/586/EY lopullinen s. 15 ja 18.

itsesääntelyä selventämällä ja varmistamalla tehokas täytäntöönpano, jättäen uusien sääntöjen kehittely taka-alalle.[22]

Direktiiviä sovelletaan kaikkiin tietoyhteiskunnan etäpalveluihin mutta ainoastaan silloin, kun palvelun tarjoaja on sijoittautunut johonkin jäsenvaltioon. Yhteisön ulkopuolelta toimiva palveluntarjoaja ei voi hyödyntää sisämarkkinoiden alueen mahdollisuuksia muuten kuin sijoittautumalla johonkin jäsenvaltioista. Direktiivillä ei ole vaikutusta Euroopan yhteisön kansainvälisiin oikeuksiin ja velvoitteisiin, eikä myöskään vaikutusta kansainvälisissä organisaatioissa käytyjen erilaisten keskustelujen tuloksiin.[23] Direktiivillä ei siis pyritä rajoittamaan kansainvälisissä järjestöissä tapahtuvaa harmonisointityötä.

Direktiivillä pyritään turvaamaan kuluttajansuojan korkea taso. Viranomaisten on suoritettava tehokasta valvontaa laittoman toiminnan alkulähteellä, pyrkimyksenä vähentää laittoman toiminnan määrää Internetissä EU:n sisämarkkinoilla. Elinkeinonharjoittajille asetetaan velvoitteita koskien tiedotusta, avoimuutta ja säädöksiä sopimussuhteen takuukeinojen[24] tarjoamisesta, jotta kuluttaja voi tehdä perusteltuja ostopäätöksiä. Kuluttajan ostopäätöksiä tuetaan myös monipuolisilla muutoksenhakukeinoilla.[25] Direktiivissä annetaan jäsenvaltiolle mahdollisuus kuluttajien suojaamiseksi ryhtyä tietyin ehdoin rajoittamaan erityisesti kuluttajien kanssa tehtävien sopimusten vapaata liikkuvuutta.[26]

Direktiivin säädöksissä käsitellään tarkemmin muun muassa sisämarkkinoita, palvelun tarjoajien sijoittautumista, kaupallista viestintää, palvelun tarjoajia koskevaan avoimuuteen ja tietojen antamiseen liittyviä vaatimuksia, sähköisessä muodossa tehtäviä sopimuksia, välittäjien vastuuta, käytännesääntöjä, muualla kuin tuomioistuimissa

---

[22] Laine (toim.) 2001 s. 8.
[23] KOM 1998/586/EY lopullinen s. 15–17.
[24] Sopimussuhteen takuukeinoilla tarkoitetaan mm. velvoitetta tarjota käyttäjille mahdollisuus korjata toimintavirheensä, verkkosopimuksen syntyhetken selkiyttäminen ja palvelun tarjoajalta edellytetty vastaanottoilmoituksen lähettäminen.
[25] Muutoksenhakukeinoilla tarkoitetaan mm. käytännesääntöjen luomista, riita-asioiden sovittelua, muutoksenhaun nopeuttamista ja tehostamista tuomioistuimissa sekä kuluttajille apua tarjoavien yhteyspisteiden perustamisesta jäsenvaltioihin.
[26] KOM 1998/586/EY lopullinen s. 18–19.

tapahtuvaa riitojen ratkaisemista, oikeussuojakeinoja ja jäsenvaltioiden viranomaisten välistä yhteistyötä.[27]

2.2.2 Direktiivi sähköisiä allekirjoituksia koskevista yhteisön puitteista

EU:ssa varsinainen direktiiviehdotus[28] koskien sähköisiä allekirjoituksia annettiin vuonna 1998. EU:n näkökulmasta silloisena riskinä oli, että erilaiset kansalliset säännökset voisivat haitata sisämarkkinoiden kehittymistä varsinkin sellaisilla aloilla, jotka ovat riippuvaisia sähköisiin allekirjoituksiin liittyvistä tuotteista ja palveluista. EU:ssa on lähdetty siitä, että sähköisiä allekirjoituksia koskeva oikeudellinen kehys on luotava yhteisötason lainsäädännön pohjalta. Taustalla oli pyrkimys välttää sisämarkkinoiden toimintahäiriöt alalla, jota Euroopan taloudessa pidettiin olennaisen tärkeänä. Yksi keskeisistä tavoitteista oli selventää sähköisten allekirjoitusten oikeudellista asemaa.[29] Jäsenvaltioiden tuli varmistaa, ettei jäsenmaan oikeusjärjestelmässä sopimuksentekomenettelyyn sovellettavilla oikeudellisilla vaatimuksilla asetettu esteitä sähköisessä muodossa tehtäville sopimuksille.[30] Toisin sanoen oli varmistettava niiden oikeudellinen sitovuus, joka asetettiin usein kyseenalaiseksi.

Euroopan parlamentti ja neuvosto antoivat direktiiviin sähköisiä allekirjoituksia koskevista yhteisön puitteista joulukuussa 1999. Direktiivissä määriteltiin sähköiset allekirjoitukset ja varmennepalvelut yhteisön alueella.

Direktiivin liitteet I-IV ovat merkittävässä asemassa määriteltäessä sähköisiin allekirjoituksiin liittyviä vaatimuksia. Direktiivin liitteessä I käydään läpi hyväksyttyjä varmenteita koskevat vaatimukset, liitteessä II hyväksyttyjä varmenteita myöntävien varmennepalvelujen tarjoajia koskevat vaatimukset, liitteessä III turvallisia allekirjoituksen luomismenetelmiä koskevat vaatimukset ja liitteessä IV turvallista

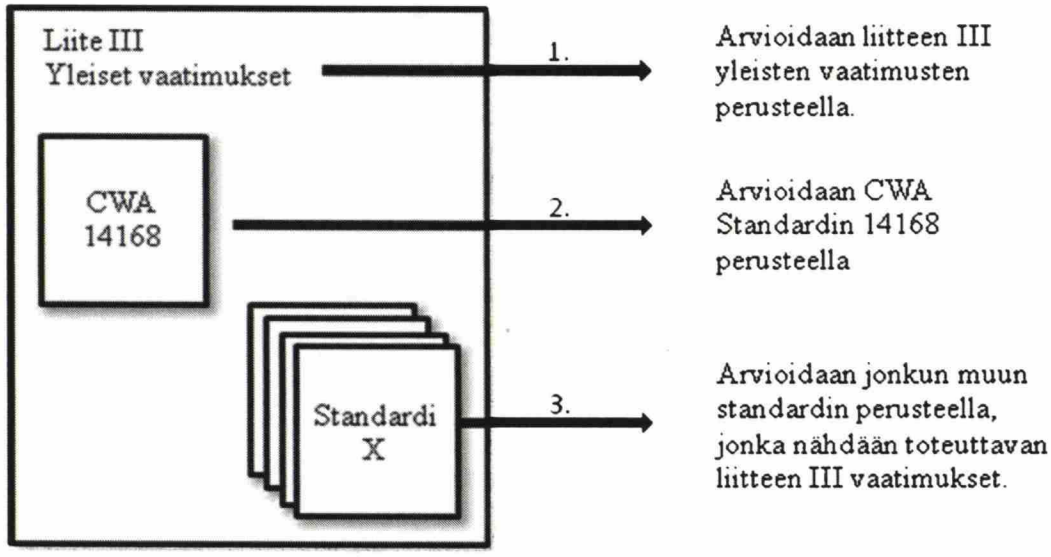
---

[27] SEK/2000/0386 lopullinen ks. kohta 2. Direktiivin tarkoitus.
[28] EYVL C 325, 23.10.1998 s. 5.
[29] KOM 2006/120/EY s. 7.
[30] Railas 2005 s. 1278.

allekirjoituksen todentamista koskevat suositukset.[31] Liitteiden vaatimuksia ja suosituksia käydään tarkemmin läpi sähköisten allekirjoitusten käsittelyn yhteydessä. Edellä mainittu liitteet I-IV löytyvät tutkielman liitteestä 1.

Direktiivin yleisiä vaatimuksia turvallisille sähköisille allekirjoituksille tarkentaakseen on Euroopan standardointikomitea CEN (Comité Européen de Normalisation) julkaissut yksityiskohtaisen standardin CWA (CEN Workshop Agreement) 14169.[32] Kaikki tämän standardin tai direktiivin täyttävät sähköisen allekirjoituksen luomisvälineet voidaan siis nähdä EU:n juridisesti hyväksymiksi sähköisen allekirjoituksen luomisvälineiksi.[33]

Jäsenvaltioilla on käytännössä kolme vaihtoehtoista menetelmää turvallisten allekirjoitusten luomismenetelmien vaatimustenmukaisuuden arvioinnille:



Kuvio 1: Vaihtoehtoiset menetelmät turvallisten allekirjoitusten luomisvälineiden vaatimustenmukaisuuden arvioinnille[34]

---

[31] 99/93/EY liitteet I-IV
[32] Liikenne- ja viestintäministeriö 2005a s. 6.
[33] Liikenne- ja viestintäministeriö 2005a s. 6.
[34] Liikenne- ja viestintäministeriö 2005a s. 12.

2.2.3 Muut direktiivit

Direktiivissä teknisiä standardeja ja määräyksiä ja tietoyhteiskunnan palveluja koskevia määräyksiä koskevien tietojen toimittamisessa noudatettavasta menettelystä rajoitetaan merkittävästi jäsenvaltioiden oikeutta säätää tietoyhteiskunnan palveluista yhteisölainsäädännöstä poikkeavaa kansallista lainsäädäntöä. Direktiivi mahdollistaa yhteisön valvonnan koskien jäsenvaltioiden tietoyhteiskunnan palveluja ja erityisesti voidaan keskittyä valvomaan sisämarkkina-alueen uusien palveluiden tarjonnan- sekä sijoittautumisvapaudenperiaatetta.[35]

Direktiivin mukaan jäsenmaiden tulee noudattaa ilmoitusmenettelyä, jonka avulla jäsenmaat tiedottavat ja kuulevat vastavuoroisesti toisiaan sekä komissiota. Ilmoitusmenettely tulee suorittaa ennen kuin jäsenmaat hyväksyvät kansallisia tietoyhteiskunnan palveluja koskevia määräyksiä.[36] Direktiivi on implementoitu kansalliseen lainsäädäntöön teknisiä määräyksiä koskevien tietojen toimittamisesta noudatettavasta menettelystä annetulla valtioneuvoston päätöksellä (802/1999).

Direktiivissä kuluttajansuojasta etäsopimuksissa säädellään kuluttajien ja elinkeinonharjoittajien välistä verkkokauppaa koskevia keskeisiä sopimusoikeudellisia periaatteita. Direktiiviä käsitellään tarkemmin tutkielman osassa etäsopimuksien luonne ja kuluttajansuoja luvussa 3.2.

2.3 Kansallinen sääntely

Suomen sopimusoikeus rakentuu lähinnä pohjoismaisten esikuvien mukaan 1929 syntyneen oikeustoimilain ja oikeuskäytännön varaan. Toistakymmentä vuotta sitten oikeustoimilain uudistamisen yhteydessä todettiin, että viestinsiirtotekniikan kehitys ei tuonut sellaisia keskeisiä ilmiöitä, jotka olisivat edellyttäneet muutoksia lakiin.[37]

---

[35] Laine (toim.) 2001 s. 7.
[36] Työ- ja elinkeinoministeriö. Ks. http://www.tem.fi/index.phtml?s=532.
[37] Ks. oikeustoimilakitoimikunnan mietintö KOM 1990:20 s 76.

Suomen sopimusoikeudellisessa lainsäädännössä ei siis tunnetta käsitettä sähköinen sopimus.

Suomessa sähköisiä sopimuksia sääntelevä kansallinen lainsäädäntö on lähes poikkeuksetta annettu implementoimalla Euroopan parlamentin ja neuvoston direktiivit Suomen kansalliseen lainsäädäntöön. Kansallisessa lainsäädännössä direktiivien säädökset on sisällytetty muun muassa lakiin sähköisistä allekirjoituksista (24.1.2003/14), lakiin tietoyhteiskunnan palvelujen tarjoamisesta (5.6.2002/458), kuluttajansuojalakiin (20.1.1978/38), lakiin sähköisestä asioinnista viranomaistoiminnassa (1.2.2003/13) sekä teknisiä määräyksiä koskevien tietojen toimittamisesta noudatettavasta menettelystä annetulla valtioneuvoston päätöksellä (802/1999).

Laki sähköisistä allekirjoituksista pyrkii edistämään sähköisten allekirjoitusten käyttöä ja niihin liittyvien tuotteiden ja palveluiden tarjontaa sekä sähköisen kaupankäynnin ja sähköisen asioinnin tietosuojaa ja tietoturvaa.[38]

Lailla tietoyhteiskunnan palvelujen tarjoamisesta säädetään erityisesti sähköisten palveluiden tarjoamisen vapaudesta, palveluiden tarjoajien velvollisuudesta antaa tietoja, sopimusta koskevien muotovaatimusten täyttämisestä sähköisesti sekä välittäjinä toimivien palvelun tarjoajien vastuuvapaudesta.[39]

Laissa kuluttajansuojasta säädetään yleisistä kuluttajanoikeuksista, joita sovelletaan myös sähköisessä kaupassa. Kuluttajansuojalain luvussa viisi käsitellään yleisiä säädöksiä kuluttajakaupasta joita sovelletaan Internetin välityksellä tapahtuvaan tavaroiden kuluttajakauppaan. Luvun kuusi säännökset koskevat etäsopimuksia eli sopimuksia jotka tehdään tietoverkkoa tai muuta etäviestintä käyttäen ilman että sopimusosapuolet ovat yhtä aikaa läsnä. EY:n perustamissopimuksen mukaan Suomella on oikeus toteuttaa ja pitää voimassa direktiivejä parempaa kuluttajansuojan tasoa

---

[38] Laki sähköisistä allekirjoituksista (24.1.2003/14) 1 §.
[39] Laki tietoyhteiskunnan palvelujen tarjoamisesta (5.6.2002/458) 1 §.

edellyttäen, että tämä on sopusoinnussa perustamissopimuksen määräysten kanssa.[40] Suomen kuluttajansuojalaki takaa tietyissä kysymyksissä korkeamman suojan kuluttajalle kuin EU-direktiivit vaativat.

Lailla sähköisestä asioinnista viranomaistoiminnassa pyritään edesauttamaan sähköisen asioinnin sujuvuutta viranomaisasioissa, tietoturvaa hallinnossa, tuomioistuimissa ja muissa lainkäyttöelimissä sekä ulosotossa.[41]

Valtioneuvoston päätöksessä teknisiä määräyksiä koskevien tietojen toimittamisesta noudatettavasta menettelystä säädetään valmistelevan viranomaisen ilmoitusvelvollisuudesta Euroopan yhteisöjen komissiolle koskien uusia ja muutettavia teknisiä määräyksiä koskevista ehdotuksista. Ilmoitus tietoyhteiskunnan palveluja koskevista uusista tai muutettavista teknisistä määräyksistä tehdään kauppa- ja teollisuusministeriön kautta.[42]

---

[40] Laine 1998 s. 15.
[41] Laki sähköisestä asioinnista viranomaistoiminnassa (1.2.2003/13) 1 §.
[42] Valtioneuvoston päätös teknisiä määräyksiä koskevien tietojen toimittamisesta noudatettavasta menettelystä (802/1999) 1:1.

3. Sähköisen sopimuksen syntyminen ja sitovuusperusteet

Suomessa perinteisen sopimuksen on katsottu syntyvän, kun ostaja hyväksyy myyjän tarjouksen. Pätevä sopimus on siten edellyttänyt tarjousta ja siihen annettua hyväksyvää vastausta. Jos vastaus on asettanut lisäehtoja kaupan toteutumiselle, tämä on katsottu vastatarjoukseksi, joka taas on edellyttänyt vastapuolen hyväksyntää. Jos sopimuksen syntymistä edeltää monivaiheiset sopimusneuvottelut, on käytännössä mahdotonta eritellä osapuolten esittämiä tarjouksia ja vastauksia. Tällöin sopimus syntyy vasta, kun sopimus on allekirjoitettu tai osapuolet muuten katsovat sopimuksen syntyneen.[43]

Yleisesti sopimusoikeuden normit soveltuvat riippumatta sopimuksen muodosta. Tästä johtuen lähes kaikki sopimusoikeudelliset kysymyksenasettelut saattavat tulla ajankohtaiseksi myös sähköisesti solmitun sopimuksen osalta. Tahdonilmaisun vastaanottajalla on riski siitä, että viestin lähettäneellä osapuolella ei ole oikeutta oikeustoimen tekemiseen tai osapuoli ei ole se, joka väittää olevansa. Tahdonilmaisun vastaanottajan tulee ratkaista onko tahdonilmaisun antaja identifioinut itsensä vastaanottajalle tarpeeksi riskittömällä tavalla.[44]

Sähköiset sopimukset voidaan jaotella kolmeen eri kategoriaan tarkastelemalla sopimusosapuolten aktiivisuutta ja passiivisuutta sopimusmenettelyn aikana. Ensimmäisessä kategoriassa sopimuksen syntyminen edellyttää molempien sopijapuolten oma-aloitteista toimintaa sopimusmenettelyn aikana. Sopimus syntyy molempien osapuolten nähtävissä olevista tarjouksesta ja vastauksesta, jotka välitetään sopimuksen osapuolille sähköisesti esimerkiksi sähköpostia käyttämällä.[45]

---

[43] Nurmi 1997 s. 23–24.
[44] www.tieke.fi / Julkaisut / Oppaat yrityksille / Sähköisen kaupankäynnin aapinen / sähköisen kaupankäynnin oikeudelliset kysymykset / Yritysten välisen sähköisen kaupan oikeudellisia kysymyksiä, 11.2.2008.
[45] Nurmi 1997 s. 11.

Toisessa kategoriassa sopijapuoli toimii aktiivisesti sopimusmenettelyssä passiivisen vastapuolen antaessa sopimuksen syntymiseen johtavat tahdonilmaisut sähköisesti ennalta ohjelmoidulla tavalla. Kyseisen kategorian sähköiset sopimukset muodostavat yleisesti tunnetuimman sähköisen kaupan muodon, johtuen kyseisten sopimusten laaja-alaisesta käytöstä verkkokaupankäynnissä.[46]

Kolmannessa kategoriassa sopimus syntyy tietokoneiden välillä automaattisesti EDI-sopimusmenettelyllä (Electronic Data Interchange[47]). EDI-sopimusmenettely ei vaadi sopijapuolten aktiivista osallistumista varsinaisen sopimuksen tekemiseen.[48] Olennaista kyseisen kategorian sähköissä sopimuksissa on ennalta sovitussa muodossa toteutettavan sopimusprosessin konekielisyys ja automaattisuus sekä sopimusprosessin sitovuus ilman ihmisten aktiivista sopimusprosessiin puuttumista.[49] EDI-sopimuksia käytetään lähinnä yritysten välisessä keskinäisessä kaupassa. Tässä tutkielmassa ei käsitellä kahden tai useamman tietokoneen välisiä konekielisiä automatisoidusti syntyviä EDI-sopimuksia.

3.1 Tarjous–vastaus -mekanismin soveltuvuus sähköisiin sopimuksiin

Sopimuksen on katsottu perinteisesti syntyvän kun myyjä saa antamaansa tarjoukseen hyväksyvän vastauksen ostajalta, kuten 1 §:ssä laissa varallisuusoikeudellisista oikeustoimista (OikTL, 228/1929) säädetään. Sopimuksentekotapojen muutokset ja sopimusneuvotteluiden monimutkaistuminen ovat vähentäneet perinteisen tarjous–vastaus -mekanismin soveltamisalaa, koska OikTL:n sopimusmekanismi ei tarjoa riittävää perustaa sopimuksen syntykysymysten arvioinnille.[50] Tarjous–vastaus -malli on suomalaisessa oikeusjärjestyksessä kuitenkin edelleen sopimuksen tekemisen lähtökohtamalli.[51] Sähköisten sopimusten yleistyminen on kuitenkin lisännyt tarjous–vastaus -mekanismin merkitystä, sillä sähköisten sopimusten syntymistä ei useinkaan

---

[46] Nurmi 1997 s. 11.
[47] EDI on suomeksi OVT (Organisaatioiden välinen tiedonsiirto).
[48] Baum – Perritt 1991 s. 2.
[49] Nimmer 1996 s. 211.
[50] Hemmo 2003 s. 97.
[51] Nurmi 1997 s. 11.

edellä monimutkaiset sopimusneuvottelut, vaan tavallisesti sopimussuhteen edellyttämä yksimielisyys syntyy vuoroittaisten sähköisten tahdonilmaisujen avulla.[52]

Oikeustoimilain säädösten ollessa dispositiivista lainsäädäntöä (OikTL 1 §) on muistettava, että tarjous–vastaus -mekanismi ei ole pakottavaa lainsäädäntöä vaan siitä voidaan poiketa osapuolten välisillä sopimuksilla, kauppa- tai muun tavan perusteella. Oikeustoimilain säännökset eivät myöskään koske määrämuotoisia sopimuksia (OikTL 1.2 §).

Tarjouksen tekijää sopimus sitoo tarjouksen antamishetkestä alkaen aina annetun määräajan loppuun saakka siinä tapauksessa, että se hyväksytään. OikTL 7 §:n mukaan ratkaiseva ajankohta tahdonilmaisusidonnaisuuden kannalta on vastaanottajan selonottohetki.[53] Tarjouksen peruuttaminen on mahdollista ainoastaan ennen, kun vastaanottaja on ottanut siitä selon, sillä tämän jälkeen tarjoussidonnaisuus on voimassa.

Kieltäytyessään tarjouksen mukaisesta toimenpiteestä, sen antaja syyllistyy sopimusrikkomukseen, mistä seuraa sanktio. Muutamia poikkeuksiakin kuitenkin on; tarjoussidonnaisuuden voi lakkauttaa yllättävä suoritusestetyyppinen tapahtuma, joka johtaisi valmiin sopimuksen raukeamiseen tai vähintään velvoitteiden olennaiseen muuttumiseen. Tällaisen tapahtuman kriteerit ovat kuitenkin tiukat ja esimerkiksi tarjouksen tekijän kuolema ei välttämättä johda sidonnaisuuden lakkaamiseen.[54]

Tarjoukseen sisältyy usein määräaika, jonka sisällä hyväksyvä vastaus on annettava (OikTL 2.1 §). Jollei aikaa ole annettu, tulee vastaus antaa kohtuullisessa ajassa tarjouksen saapumisesta (OikTL 3.2 §).[55] Tästä poikkeuksena on suullinen tarjous, johon vastaus tulee antaa välittömästi tai se raukeaa (OikTL 3.1 §).[56] On myös keskusteltu siitä, mikä sähköisessä sopimuksenteossa on kohtuullinen aika. Koska toiminta verkossa on yleisesti erittäin nopearytmistä, onko tällöin 'kohtuullinen aika'

---

[52] Hemmo 2003 s. 97.
[53] Hemmo 2003 s. 101.
[54] Hemmo 2003 s.101.
[55] Hoppu – Hoppu 2007 s. 51.
[56] Hoppu – Hoppu 2007 s. 52.

lyhyempi kuin muita kanavia käytettäessä?[57] On esitetty, että puhelimessa esitetty tarjous on rinnastettavissa suulliseen tarjoukseen. Onko tällä ajattelutavalla myös esim. sähköposti verrattavissa suulliseen tarjoukseen, sillä viestin kulkemiseen kuluva aika on käytännöllisesti katsoen olematon? Tosin tällöin on mahdotonta tietää, ovatko molemmat osapuolet samanaikaisesti läsnä, sillä viesti säilyy vastaanottajalla vaikka hän ei siitä heti ottaisikaan selkoa. Tämä vaikeuttaa oikeusvaikutuksen alkamisajan selvittämistä. Teknologian kehittymisen myötä erilaisten sähköpostijärjestelmien ominaisuudet ovat kuitenkin lisääntyneet, ja nykyään tietyissä sisäisissä järjestelmissä lähettäjän on myös mahdollista saada tieto siitä kun viesti on vastaanotettu ja erikseen kun se on luettu. Vasta kun kyseiset toiminnot yleistyvät tarpeeksi, voidaan niitä alkaa soveltaa oikeuskäytännössä.[58]

Mikäli vastaus saapuu myöhässä, käsitetään se uudeksi tarjoukseksi ja on ensimmäisen tarjouksen antajan harkinnassa hyväksyykö hän sopimuksen syntymisen.[59] Hylätty tarjous raukeaa välittömästi (OikTL 1-5§). Oikeusvaikutuksen alkamista määrittävät kolme eri teoriaa: lähettämisteoria, jonka mukaan oikeusvaikutus alkaa tahdonilmaisun lähettämishetkellä; saapumisteoria, jonka mukaan vaikutus alkaa kun ilmaisu on saapunut vastaanottajalle sekä selonottoteoria jonka mukaan vaikutus alkaa kun vastaanottaja on ottanut siitä selon. Eri tilanteissa sovelletaan eri teorioita ja ne täydentävät toisiaan oikeuskäytännössä. Konkreettisena saapumishetkenä pidetään kuitenkin yleensä sitä ajankohtaa, jolloin vastaanottajalla on tavallisissa olosuhteissa ollut mahdollisuus ottaa ilmaisusta selko.[60]

Laissa tietoyhteiskunnan palvelujen tarjoamisesta täsmennetään, että etäpalvelujen osalta palvelua koskeva tilaus ja vastaanottoilmoitus katsotaan vastaanotetuiksi kun ne ovat adressaatin käytössä (TietoyhtPalvL 11 §). Lain mukaan etäpalvelujen osalta tilaus ja vastaanottoilmoitus katsotaan vastaanotetuksi, kun viesti on vastaanottajan käytettävissä. Saapumisajankohdaksi katsotaan viestin saapumisaika

---

[57] Hemmo 2003 s. 104.
[58] Nurmi 1997 s. 45–52.
[59] Hoppu – Hoppu 2007 s. 52.
[60] Hoppu – Hoppu 2007 s. 50.

sähköpostilaatikkoon riippumatta siitä, milloin viesti tosiasiallisesti avataan.[61] Oikeustoimilain *Re integra* –periaatteen (OikTL 39 §) mukaan ratkaisevaa määräaikaa voidaan siirtää, jos erityiset asianhaarat antava siihen aihetta, siihen asti kunnes tahdonilmaisu on vaikuttanut määräävästi vastaanottajan toimintaan.[62]

On kuitenkin tärkeää erottaa toisistaan tarjous ja kehotus ostotarjouksen tekemiseen. Yritykset mainostavat usein kotisivuillaan tuotteita, joita on mahdollista hankkia sen kautta. Mikäli sivuilla on tarkat tuotetiedot ja hinnat kyseisille kohteille, kuluttajalle syntyy helposti mielikuva, että sivu on luokiteltavissa tarjoukseksi ja yrittäjä sitoutuu toimittamaan kyseisen tuotteen kyseisellä hinnalla. Koska esimerkiksi Internetin kautta tapahtuvassa markkinoinnissa mahdollisena kohderyhmänä voi kuitenkin olla käytännöllisesti katsoen satoja tuhansia ellei jopa miljoonia ihmisiä, tuotteensa kilpailukykyisesti hinnoittelevan myyjän ongelmana voi olla tavaran riittävyys. Siksi myyjän olisikin suositeltavaa ilmoittaa sivulla, että kyse ei ole tarjouksesta vaan potentiaalisille asiakkaille suunnatusta kehotuksesta ostotarjouksen tekemiseen.[63]

Tarjouksen tunnusmerkkinä on pidetty kohdistumista rajattuun henkilöpiiriin, ja tällä perusteella esimerkiksi tv-mainoksia ja kotisivuja ei voisi pitää sitovina tarjouksina.[64] Lisäksi on edellytetty sellaista sisällön konkretisointia, että tarjous voi muodostaa perustan tulevalle sopimukselle, mikä tosin yleensä täyttyy ainakin markkinointiin tarkoitetulla verkkosivustolla. Myös kapasiteettikysymystä on käytetty määrittämään tarjoussidonnaisuutta; mikäli vastaanottajan olisi pitänyt ymmärtää, ettei sopimuksia voida täyttää rajatonta määrää, ei hänellä ole oikeutta tulkita ilmoitusta tarjoukseksi.[65] Lyhyesti voidaan kuitenkin todeta, että oikeuskäytäntö tuntee kehotuksen tarjouksen tekemiseen, ja yleensä rajaamattomalle joukolle tehtyjä ilmoituksia ei voida katsoa sitoviksi.[66]

---

[61] Hemmo 2003 s. 102. Ks. HE 194 / 2001 11 §:n perustelut.
[62] Hemmo 2003 s. 102.
[63] http://www.ebusinesslex.net/front/dett_art.asp?idtes=95.
[64] Hoppu – Hoppu 2007 s. 55.
[65] Hemmo 2003 s. 108.
[66] Hemmo 2003 s. 107.

Mikäli myyjän ilmoitusta sellaisenaan ei katsota tarjoukseksi, vaan ainoastaan kehotukseksi vastaanottajalle, sopimus ei synny vielä ainoastaan toisen osapuolen lähettäessä ostotarjouksensa. Tällöin myyjän pitää vielä vahvistaa halukkuutensa sopimukseen lähettämällä asiakkaalle hyväksyvä vastaus tämän tarjoukseen.[67] Laki tietoyhteiskunnan palvelujen tarjoamisesta edellyttääkin, että ostajan tulee saada tilausvahvistus, missä tulee mainita sopimuksen olennaiset tiedot. Mikäli kyseisessä tilausvahvistuksessa on asiakkaan mielestä jotain poikkeavaa alkuperäiseen tilaukseen verrattuna, hänen tulee reklamoida siitä. Muuten tilaus jää voimaan sellaisenaan.

Lähtökohtana on, että palvelun tarjoajan ilmoittama myyntihinta sitoo häntä, mikäli ilmoitus katsotaan tarjoukseksi ja myyjä on sen sellaiseksi tarkoittanut esimerkiksi julkistamalla sen verkkokaupassaan. Kun tarjoaja myy erityisen pientä erää tuotetta erityisen halvalla, tuotteen rajallisuus on syytä mainita tarjouksessa, sillä muuten korvausvastuun syntyminen on mahdollista.[68] Poikkeuksena on, että virhe annetussa hinnassa on niin ilmeinen, että vastapuolen olisi pitänyt se ymmärtää. Tällainen virhe voisi olla esimerkiksi pilkun väärä paikka. Sähköisessä kaupankäynnissä prosessia yksinkertaistava seikka on kuitenkin se, että hinta- ja tuotetietojen pitäminen reaaliaikaisina on mahdollista ja tehdyt virheet voidaan korjata suhteellisen nopeasti. Tällöin pystytään usein minimoimaan vahingot melko pienin kustannuksin.

3.2 Etäsopimuksien luonne ja kuluttajansuoja

Verkossa syntyvät sopimukset kuuluvat etäsopimuksiin, joilla tarkoitetaan sopimuksia joiden tekemiseen palveluiden tarjoaja käyttää yksinomaan etäviestintävälineitä ennen sopimuksen tekemistä ja sopimuksen tekemisen yhteydessä. Käsitteellä etämyynti tarkoitetaan kulutushyödykkeiden tarjoamista ja markkinoimista etäviestimillä. Tietoverkkojen lisäksi etäviestimellä voidaan tarkoittaa myös mm. puhelinta, postia, televisiota tai muuta välinettä, jota käyttäen osapuolet voivat tehdä sopimuksen olematta yhtä aikaa läsnä.[69] Kuluttajan ja elinkeinonharjoittajan välisiä sopimuksia säätelee

---

[67] Laine (toim.) 2001 s. 227.
[68] Hemmo 2003 s.108.
[69] KSL 6:4.

direktiivi kuluttajansuojasta etäsopimuksissa jonka kohteena voivat olla sekä tavarat että palvelut. Etämyyntisäännöksiä ei kuitenkaan sovelleta esimerkiksi kiinteää omaisuutta koskeviin sopimuksiin.

Rahoituspalvelut eivät kuulu kyseisen direktiivin alle, vaan niitä sääntelee direktiivi kuluttajille tarkoitettujen rahoituspalveluiden etämyynnistä (2002/65/EY). Se vastaa kuitenkin sisällöltään hyvin pitkälti etäsopimusdirektiiviä, tosin ottaen huomioon alaan liittyvät erityispiirteet. Suurimpana erona on, että rahoituspalveludirektiivi pyrkii totaaliharmonisointiin, kun taas kuluttajansuojaa koskevat direktiivit yleisesti velvoittavat vain minimiharmonisointiin.[70]

Direktiivi kuluttajansuojasta etäsopimuksissa kattaa vain osan etämyyntiin ja etäsopimuksiin liittyvistä oikeudellisista kysymyksistä. Direktiivissä ei oteta esimerkiksi ollenkaan kantaa sitovan sopimuksen syntymiseen, sopimusrikkomuksiin tai niiden seuraamuksiin. Myös peruuttamisoikeuden tarkemmat oikeusvaikutukset on jätetty kansallisten lakien varaan.[71] Direktiivin implementoinnissa Suomen kansalliseen lainsäädäntöön lähtökohtana on ollut, ettei kuluttajansuojalakiin tehdä sellaisia muutoksia, jotka selvästi heikentäisivät kuluttajan oikeudellista asemaa.[72]

Verkossa syntyviin suomalaisen kuluttajan ja suomalaisen elinkeinoharjoittajan välisiin sähköisiin sopimuksiin sovelletaan kuluttajansuojalakia (KSL 38/1978). KSL:n säädösten ollessa pääosin pakottavia, elinkeinonharjoittajan ja kuluttajan välisissä sopimuksissa olevat KSL:n vastaiset ehdot ovat aina pätemättömiä ja ne korvataan KSL:n säännöksillä. EU:n sisällä tapahtuvassa kuluttajakaupassa perusperiaatteena[73] on noudattaa kohdemaan eli kuluttajan kotimaan lainsäädäntöä.[74] Maailmanlaajuisessa sähköisessä kuluttajakaupassa toimivaa yhtenäistä sääntelyä ei vielä käytännössä ole

---

[70] Minimiharmonisoinnissa jäsenvaltio saa halutessaan säätää lakeja tiukemmiksikin, ja direktiivi asettaa siis vain alimman tason. Totaaliharmonisoinnissa kaikkien jäsenvaltioiden lakien tulee olla vastaavat.
[71] HE 79/2000 kohta 4.1.1 Direktiivin vähimmäistason ylittävien säännösten vaikutus kansainväliseen sähköiseen kaupankäyntiin.
[72] HE 79/2000 kohta 4.1.1 Direktiivin vähimmäistason ylittävien säännösten vaikutus kansainväliseen kaupankäyntiin.
[73] Poikkeuksia esimerkiksi markkinoinnin osalta.
[74] HE 79/2000 kohta 4.1.1 Direktiivin vähimmäistason ylittävien säännösten vaikutus kansainväliseen kaupankäyntiin ja www.tieke.fi / Julkaisut / Oppaat yrityksille / Sähköisen kaupankäynnin aapinen / Sähköisen kaupankäynnin oikeudelliset kysymykset / Kansainvälinen kuluttajakauppa, 12.02.2008.

mutta esimerkiksi Organization for Economic Cooperation and Development (OECD) ja ICC ovat luoneet ohjesääntöjä[75], joiden avulla pyritään harmonisoimaan kansainvälistä kuluttajakauppaa.[76]

Sähköisten sopimusten luonteen vuoksi kuluttaja ei pääse näkemään itse tuotetta ja tekemään havaintoja siitä, joten hänelle tulee antaa riittävät tiedot ostopäätöksen tekemisen tueksi. Elinkeinonharjoittajalla on kaksivaiheinen tiedonantovelvollisuus; perustiedot itse elinkeinonharjoittajasta, tarjotusta hyödykkeestä, sopimusehdoista, tarjouksen kestosta ja kuluttajan peruuttamisoikeudesta on annettava jo ennen sopimuksen tekemistä (KSL 6:13) kun taas sopimuksen teon jälkeen edellä mainitut tiedot sekä niitä täydentävät tiedot tulee vahvistaa kirjallisesti tai sähköisesti (KSL 6:14) siten, että "tietoja ei voida yksipuolisesti muuttaa ja ne säilyvät kuluttajan saatavilla".[77]

Toimituksen tulee tapahtua kuluttajalle viimeistään 30 päivän kuluessa tilauksen tekohetkestä.[78] Puutteellisten tietojen takia kuluttajalle pitää myös taata peruuttamisoikeus, josta aiheutuvat välittömät kulut tulee korvata täysimääräisinä. Direktiivin vaatima peruutusaika on 7 päivää[79], mutta KSL 6:15:ssä sitä on pidennetty 14 päivään. Aika alkaa kulua siitä, kun sekä tuote että tilausvahvistus on vastaanotettu. Mikäli toinen siis saapuu myöhemmin, ajan kuluminen katsotaan alkavaksi tästä hetkestä. Tilausvahvistuksella on keskeinen osa peruuttamisoikeutta tarkasteltaessa. Jos tilausvahvistus on puutteellinen, kuluttajan peruuttamisoikeus pitenee kolmeen kuukauteen[80]. Jos tilausvahvistusta ei lainkaan anneta, sopimus sitoo ainoastaan elinkeinonharjoittajaa. Sitomattomuus on kuitenkin rajattu yhteen vuoteen; jos kuluttaja ei tänä aikana vetoa siihen, tulee sopimus myös häntä sitovaksi.[81] Peruuttamisoikeutta

---

[75] OECD:n ohjeet kuluttajansuojasta sähköisessä kaupankäynnissä, ks. http://www.oecd.org/findDocument/0,2350,en_2649_37441_1_119820_1_1_37441,00.html, 12.2.2008. ICC:n kansainväliset suositukset Internet-mainonnasta, ks. http://www.iccwbo.org/id929/index.html, 12.2.2008.

[76] Ks. www.tieke.fi / Julkaisut / Oppaat yrityksille / Sähköisen kaupankäynnin aapinen / Sähköisen kaupankäynnin oikeudelliset kysymykset / Kansainvälinen kuluttajakauppa, 12.02.2008.

[77] HE 79/2000 kohta Yksityiskohtaiset perustelut: 6. luku. Kotimyynti ja etämyynti: 14 §.

[78] HE 79/2000 kohta 3.1.7 Muut ehdotukset.

[79] HE 79/2000 kohta 1.2.1 Kuluttajan oikeus peruuttaa sopimus.

[80] HE 79/2000 kohta 3.1.4 Kuluttajan oikeus peruuttaa sopimus.

[81] Laine (toim.) 2001 s.237.

on kuitenkin rajoitettu joissakin tilanteissa, esimerkiksi elintarvikkeiden ja erityisesti kuluttajaa varten valmistettujen tuotteiden kohdalla.[82]

Elinkeinonharjoittajalla on myös velvollisuus vastata peruutuksen johdosta palautettavien tuotteiden palautuskuluista[83], jos tuote voidaan palauttaa tavanomaisella tavalla postilla (KSL 6:17). Sen sijaan jos tuote kokonsa tai painonsa takia edellyttää erilliskäsittelyä tai muuta erityiskuljetusta, palautuskuluista vastaa kuluttaja. Kuluttajan vastuulla on kuitenkin se, että peruutustapauksessa hänen on palautettava vastaanotettu tavara tai muu palautettavissa oleva suoritus kohtuullisen ajan kuluessa elinkeinonharjoittajalle.

3.3 Yritysten väliset sähköiset sopimukset

Yritysten välistä kauppaa ei pääsääntöisesti säännellä pakottavan lainsäädännön avulla vaan sopimusvapauden ja muotovapauden perusteella yritykset voivat sopia noudattavansa oikeustoimilain dispositiivisia säännöksiä tai sopia keskinäiseen suhteeseensa sovellettavista oikeuksista ja velvollisuuksista, sähköisen sopimuksen ollessa oikeudellisesti samassa asemassa kuin perinteinenkin sopimus.[84] Sopimusvapauden pohjalta solmittavissa yritysten välisissä sähköisissä sopimuksissa voi olla huomattavasti tapauskohtaisempia ja spesifisempiä oikeudellisia ongelmia verrattuna esimerkiksi kuluttajan ja elinkeinonharjoittajan väliseen kauppaan. Lainsäädännön ollessa puutteellista voivat yritykset päättää esimerkiksi UNCITRAL:in yleissopimuksen soveltamisesta keskinäisissä kansainvälisissä sopimussuhteissaan.[85]

Laissa tietoyhteiskunnan palvelujen tarjoamisesta (458/2002) säännellään etäpalveluina sähköisessä muodossa toimitettavista palveluista. Erityisesti lain kolmannessa luvussa

---

[82] HE 79/2000 kohta 3.1.2 Soveltamisala.
[83] Suomen lainsäädäntö on poikkeuksellista Euroopassa. Direktiivin täytäntöönpanon yhteydessä vastaava velvollisuus on otettu ainoastaan Saksan uuteen etämyyntilakiin. Ks. HE 79/2000 kohta 3.1.4 Kuluttajan oikeus peruuttaa sopimus.
[84] Ks. www.tieke.fi / Julkaisut / Oppaat yrityksille / Sähköisen kaupankäynnin aapinen / sähköisen kaupankäynnin oikeudelliset kysymykset / Yritysten välisen sähköisen kaupan oikeudellisia kysymyksiä, 11.2.2008.
[85] Railas 2005 s. 1290.

käsitellään yritysten välisen sähköisen kaupankäynnin kysymyksiä koskien tiedonantovelvollisuutta(7 ja 8 §), sopimusehtojen toimittamista (9 §) ja muotovaatimuksia (12 §) sekä tilaus- ja vastaanottoilmoituksia (10 §).

Tehtäessä yritysten välisiä sähköisiä sopimuksia tulisi huomiota kiinnittää siihen, miten oikeustoimet voidaan jälkikäteen todistaa. Erityisesti tulisi huolehtia sähköisten sopimusten muuntumattomuuden turvaamisesta.[86]

---

[86] Ks. www.tieke.fi / Julkaisut / Oppaat yrityksille / Sähköisen kaupankäynnin aapinen / sähköisen kaupankäynnin oikeudelliset kysymykset / Yritysten välisen sähköisen kaupan oikeudellisia kysymyksiä, 11.2.2008.

4. Sähköinen allekirjoitus

Sähköistä allekirjoitusta voidaan hyödyntää kaikenlaisen digitaalisen sisällön todentamiseen, esimerkiksi sähköpostiviestien, ohjelmistojen ja www-sivujen alkuperän selvittämiseen ja eheyden turvaamiseen.[87] Luonnolliset sekä oikeushenkilöt voivat käyttää sähköistä allekirjoitusta omakätisen allekirjoituksen asemasta. Euroopan parlamentin ja neuvoston direktiivissä sähköisistä allekirjoituksia koskevista puitteista pyrittiin luomaan edellytykset sähköisiin allekirjoituksiin liittyvien tuotteiden ja palveluiden vapaaseen liikkuvuuteen rajojen yli ja varmistamaan sähköisen allekirjoituksen oikeudellinen perusasema.[88]

Sähköinen allekirjoitus määritellään direktiivissä sähköisessä muodossa olevaksi tiedoksi, joka on liitetty tai joka loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään todentamisen välineenä. Sähköinen allekirjoituksen avulla allekirjoittajan henkilöllisyys tulee voida todeta ja kyseinen henkilö tulee pystyä liittämään allekirjoituksella vahvistettavaan tahdonilmaisuun, käytetystä teknologiasta riippumatta.[89]

Sähköisellä allekirjoituksella on suuri merkitys verkossa tehtävän kaupan edellyttämän turvallisuuden lisäämisessä erityisesti silloin, kun sopimus tehdään avoimessa tietoverkossa ja kun osapuolet eivät ole etukäteen sopineet tunnistamisen ja sisällön varmentamisen menettelytavoista.[90]

Sähköisiä allekirjoituksia ei vielä ole käytetty yleisesti verkossa tapahtuvassa kaupankäynnissä, koska suuri yleisö ei ole innostunut hankkimaan tarvittavia laitteita, esim. älykortteja ja niiden lukulaitteita. Tekniset standardit ja ratkaisut eivät ole myöskään yleistyneet riittävästi.

---

[87] Railas 2005 s. 1281.
[88] KOM 2006/120/EY s. 4.
[89] HE 197/2001 s. 4.
[90] Laine (toim.) 2001 s. 196.

Käsitteinä sähköinen allekirjoitus ja sähköinen henkilöllisyyden tunnistaminen tulee tässä yhteydessä erotella toisistaan. Sähköisessä allekirjoituksessa allekirjoittaja yhdistää sähköisen identiteettinsä tietosisältöön jonkin oikeustoimen tekemiseksi kun taas sähköisellä henkilöllisyyden tunnistamisella tarkoitetaan pelkästään henkilön sähköisen identiteetin ja yhteyden todelliseen identiteettiin todentamista ilman yhteyttä tietosisältöön. Laki sähköisistä allekirjoituksista ei sääntele ollenkaan sähköistä tunnistamista, mutta esimerkiksi yksityisyyden suojaa ja tietosuojaa koskevat säännökset sekä aineellisessa lainsäädännössä olevat vastuumääräykset voivat käsitellä tunnistamisvelvollisuutta. Rajanveto yleisen tulkinnan mukaan on, että jos henkilö antaa PIN-lukunsa (Personal Identification Number) eli henkilökohtaisen tunnuslukunsa tarkastaakseen pankkitietojaan, kysymys on puhtaasti tunnistamisesta. Kun PIN-luvun avulla tehdään oikeustoimi, on kysymyksessä direktiivin ja lain tarkoittama sähköinen allekirjoitus.[91]

EU:n direktiivissä sähköisiä allekirjoituksia koskevista puitteista määritellään kolmen tyyppisiä sähköisiä allekirjoituksia: sähköinen allekirjoitus laajassa merkityksessä, kehittynyt sähköinen allekirjoitus ja varmennettu sähköinen allekirjoitus.

4.1 Sähköinen allekirjoitus laajassa merkityksessä

Sähköisellä allekirjoituksella laajassa mielessä voidaan käsittää yksinkertaisimmillaan sähköpostin allekirjoittamista henkilön nimellä tai käyttäen PIN-lukua. Sähköpostin allekirjoittaminen tai salainen tunnuskoodi on yksi eniten käytetyistä sähköisen todentamisen välineistä, jolla yksilöidään ja todennetaan tietoa. Ongelmana salaisessa tunnuskoodissa tai henkilön nimellä allekirjoitetussa sähköpostissa on se, että avoimessa käyttäjäyhteisössä kyseisillä metodeilla ei voida varmentaa viestin lähettäjää eikä myöskään viestin eheyttä. Oikeustoimen kiistäminen ja asiakirjan väärentäminen jättämättä jälkiä voi olla helppoa tilanteessa, jossa vaihdannan osapuolet eivät ole

[91] Railas 2006 s. 12 ja 15.

aukottomasti tunnistettavissa ja jossa oikeustoimi ei säily kahdenkeskisenä tai luottamuksellisena.[92]

Sähköisen allekirjoituksen muotoja laajassa merkityksessä ajateltaessa sähköisen todentamisen menetelmiä ovat esimerkiksi käyttäjätunnukset ja salasanat, kertakäyttöiset salasanat, varmenteet mukaan lukien laatuvarmenteet ja biometriikka.[93]

Käyttäjätunnuksiin ja salasanoihin perustuva sähköinen todentaminen on selvästi eniten käytetty todentamismenetelmä sähköisissä palveluissa. Tämän alkeellisen sähköisen todentamisen muodon ongelmana on helppo kopioitavuus ja puuttuva salaus. Käyttäjätunnukset voidaan saada helposti selville arvaamalla, seuraamalla tai tallentamalla käyttäjän tietoliikennettä. Käyttäjät kirjoittavat usein ylös myös salasanansa.[94] Saman käyttäjätunnuksen ja salasanan käyttäminen useissa palveluissa voi myös muodostaa tietoturvariskin, koska epärehellinen palveluntarjoaja voi kokeilla oman palvelunsa käyttäjien tunnuksia ja salasanoja myös muihin palveluihin.[95]

Kertakäyttöiset salasanat kuten esimerkiksi suomalaisten pankkien laajalti tarjoamat TUPAS-pankkitunnisteet (Tunnistuspalvelu asiointipalveluntuottajille) ovat Suomessa yleisin sähköisen allekirjoituksen toteuttamismuoto. Esimerkiksi myös valtionhallinnon verkkopalveluissa voi nykyään käyttää TUPAS-pankkitunnisteiden avulla.[96] Pankkien tunnistusratkaisuja, kuten edellä mainittuja TUPAS-pankkitunnisteita valvoo Suomessa Rahoitustarkastus.[97]

Käyttäjätunnuksen yhdistäminen kertakäyttösalasanoihin poistaa salasanojen kopioimisesta, katoamisesta ja varastamisesta aiheutuvat ongelmat, koska kerran

---

[92] Terämaa (toim. Laine) 2001 s. 44.
[93] Liikenne- ja viestintäministeriö 2003 s. 11.
[94] Kuluttajatutkimuskeskus 2007 s. 4.
[95] Liikenne- ja viestintäministeriö 2003 s. 39.
[96] HST arkkitehtuurit ja liiketoimintamallit s. 9. Tarkempaa tietoa tunnistautumisesta valtionhallinnon verkkopalveluissa, Valtiovarainministeriön päivitetyssä ohjeessa VM 6/01/2003. Ohjeen periaatteena on, että sähköiseen tunnistamiseen ei ole yhtä ainoata vaihtoehtoa, vaan tunnistamisessa voidaan hyödyntää erilaisia tunnisteita.
[97] VM 40/01/2006 s. 15.

käytetystä salasanasta ei voida laskea tulevaa salasanaa.[98] Tietoturvansa puolesta se ei kuitenkaan ole juuri käyttäjätunnuksiin ja salasanoihin perustuvaa todentamista turvallisempi, koska salasanalistat tulostetaan paperille, jotka ovat helposti kopioitavissa. Ongelma syntyy, kun epärehellinen taho saa käsiinsä käyttäjätunnuksen sekä tiedon itse palvelusta, johon salasanalista ja käyttäjätunnus ovat valideja. On myös yleistä, että käyttäjät kirjoittavat käyttäjätunnuksensa salasanalistaan ja salasanalistan ulkoasusta yleensä voidaan päätellä mihin palveluun se antaa käyttöoikeuden. Teoriassa myös salasanalistan generointialgoritmin paljastuminen saattaisi mahdollistaa salasanalistojen salasanojen laskemisen.[99]

TUPAS-pankkitunnisteet eivät täytä lain sähköisistä allekirjoituksista vaatimuksia kehittyneen sähköisen allekirjoituksen osalta mutta sopimusvapaus antaa kuitenkin mahdollisuuden kertakäyttösalasanojen käyttämiseen allekirjoittamistarkoituksessa.[100] Asiakas ja pankki voivat sopia, että pankkitunnuksien avulla vahvistettava toimenpide vastaa sähköistä allekirjoitusta.[101] Vaikka TUPAS-pankkitunnisteilla tehdyt allekirjoitukset ovat saaneet kauppatapaan rinnastettavaa uskottavuutta, voidaan erityisesti kiistämisoikeus kyseenalaistaa, koska niitä ei ole oikeudellisesti testattu peruuttamattomuuden tai allekirjoitetun tietosisällön määrittelyn osalta.[102]

4.2 Kehittynyt sähköinen allekirjoitus

Kehittyneellä sähköisellä allekirjoituksella tarkoitetaan allekirjoitusta jossa käytetään julkisen avaimen järjestelmää (Public Key Infrastructure eli PKI). Kehittyneen sähköisen allekirjoituksen täytyy täyttää tiedon alkuperän todentamisen, identifioinnin, kiistämättömyyden ja eheyden vaatimukset.[103] Vaikka direktiivi sähköisiä allekirjoituksia koskevista puitteista on teknologianeutraali, kehittyneellä sähköisellä

---

[98] Kuluttajatutkimuskeskus 2007 s. 5.
[99] Liikenne- ja viestintäministeriö 2003 s. 40.
[100] HST arkkitehtuurit ja liiketoimintamallit s. 9.
[101] Männikkö 2007 s. 15.
[102] Liikenne- ja viestintäministeriö 2005b s. 19.
[103] KOM 2006/120/EY s. 4-5. Kehittyneen sähköisen allekirjoituksen on täytettävä 1999/93/EY 2 artiklan 2 vaatimuksen.

allekirjoituksella tarkoitetaan käytännössä julkisen avaimen menetelmällä tehtyjä sähköisiä allekirjoituksia.

Julkisen avaimen järjestelmän tekniikassa hyödynnetään kryptografiaa. PKI-järjestelmää voidaan käyttää sekä sähköisessä allekirjoituksessa että tiedon luottamuksellisuuden turvaamisessa. Julkisen avaimen menetelmä eli PKI perustuu kahden eri avaimen olemassaoloon. Kullekin käyttäjälle generoidaan kahdesta avaimesta koostuva avainpari. Kun avainparin toisella avaimella salataan tietoa, niin salaus voidaan purkaa ainoastaan avainparin toisella avaimella. Avaimet luodaan siten, että niitä ei voi johtaa toisistaan.[104]

Toinen avaimista on julkinen avain ja toinen yksityinen avain. Julkinen avain on julkisesti kaikkien nähtävillä kun taas yksityinen avain on ainoastaan omistajansa hallussa. Kun yksityisellä avaimella on salattu jotain tietoa, voidaan olla varmoja, että alkuperäisen tiedon salanneella taholla on ollut hallussaan avainparin yksityinen avain. Julkinen avain talletetaan yleensä julkiseen rekisteriin, minkä lisäksi se voidaan liittää lähetettyyn viestiin mukaan. Julkisen avaimen avulla varmenteeseen tukeutuvat osapuolet voivat varmistaa sähköisen allekirjoituksen olevan aito, edellyttäen että he pitävät varmentajaa luotettavana tahona.[105]

Yksityisen avaimen turvallinen säilyttäminen on PKI-järjestelmissä käyttäjän tietoturvan kannalta erityisen tärkeätä. Avain on pitkä ja sen muistaminen on käytännössä mahdotonta. Yksityinen avain on tallennettava ja suojattava, mikä huonosti toteutettuna saattaa mahdollistaa väärinkäytökset. Turvallisimpina järjestelyinä voidaan pitää älykorteille ja erillisille laitteille tallennettavia yksityisiä avaimia.[106]

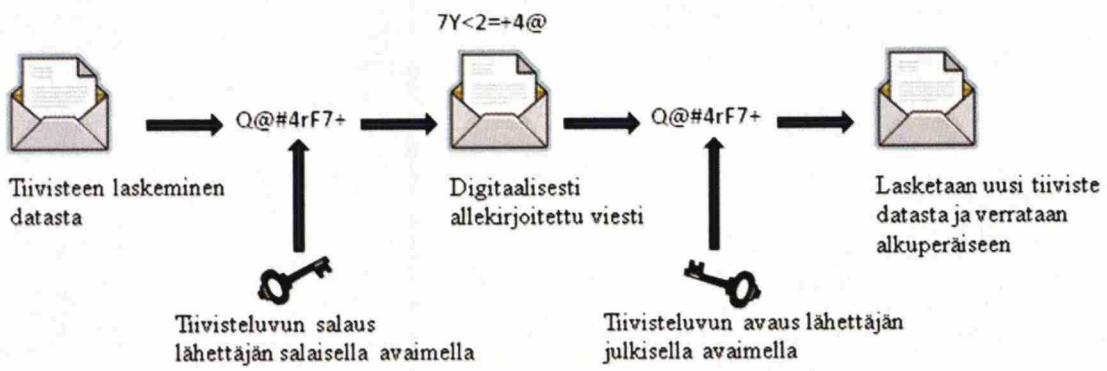
PKI-teknologiaan perustuvat varmenteet voidaan toteuttaa teknisesti monella eri tavalla, koska varmenteita voidaan tallentaa erilaisille alustoille, esimerkiksi älykorteille.[107] Älykorttina voidaan käyttää esimerkiksi henkilö- ja pankkikorttia sekä

---

[104] Laine (toim.) 2001 s. 208–209.
[105] Laine (toim.) 2001 s. 209–211.
[106] Järvinen 2003 s. 160–161.
[107] Järvinen 2003 s. 165.

matkapuhelinoperaattoreiden SIM-korttia (Subscriber Identity Module). Älykortille on mahdollista asentaa useita sovelluksia, joista PKI-toiminnallisuus ja varmenne on yksi. Salausprosessorilla ja muistilla varustettu älykortti on tietoturvallinen ja helppokäyttöinen varmenteiden säilytys- ja käsittelyalusta. Älykortilla olevia yksityisiä avaimia voidaan käyttää ainoastaan syöttämällä oikea henkilökohtainen PIN-luku. Mahdollisesti käytettävä lukijalaite ei pääse suoraan käsiksi salausavaimiin, vaan kortin prosessori hoitaa salauksen ja palauttaa vain valmiin tuloksen lukulaitteen kautta tietokoneelle. Yksityisiä avaimia ei ole mahdollista kopioida kortilta muualle, joten kortin haltijan identiteetin kopioiminen ei ole mahdollista.[108]

Yksityisen avaimen käyttö on suojattu PIN-luvulla, jonka vain kortin omistaja tietää. Kortin haltija voi tarvittaessa vaihtaa tunnuslukua. Väärän tunnusluvun syöttäminen useampaan otteeseen lukitsee kortin. Kortin ja henkilökohtaisten avainten väärinkäyttö vaatii sekä älykortin että avaimia suojaavien tunnuslukujen saamista haltuun. PIN-luvun säilyttämiseen liittyy käyttäjätunnusta ja salasanaa vastaavat tietoturvaongelmat, kuten esimerkiksi liian helppo PIN-koodi, muistilaput, kiristäminen ja uhkailu.[109] Ongelmatilanteessa henkilön varmenne voidaan viipymättä peruuttaa, jolloin kortti muuttuu käyttökelvottomaksi. Älykortin haltija on vastuussa sen väärinkäytöksistä aina tilanteessa, jossa kortinhaltija on luovuttanut kortin ja PIN-luvun tarkoituksellisesti toiselle henkilölle tai jos väärinkäytökset ovat aiheutuneet älykortin haltijan omasta huolimattomuudesta, joka ei ole lievää.[110]



Kuvio 2: Kehittyneen sähköisen allekirjoituksen muodostaminen[111]

---

[108] HST työryhmä 2003 s. 8.
[109] Liikenne- ja viestintäministeriö 2003 s. 41.
[110] HST työryhmä 2003 s. 8 ja Järvinen 2003 s. 209.
[111] Rinne 2002 kuva 38 (mukaillen) s. 89.

Digitaalinen allekirjoitus muodostetaan laskemalla tiivisteluku allekirjoitettavasta asiakirjasta. Tiivisteluku salataan allekirjoittajan yksityisellä avaimella, salauksen tuloksena on digitaalinen allekirjoitus. Se liitetään esimerkiksi allekirjoitetun sähköisen asiakirjan perään. Taho joka haluaa tarkistaa sähköisen allekirjoituksen, avaa lähettäjän tiivisteluvun julkisella avaimella, laskee itse uuden tiivisteluvun ja vertaa näitä kahta tiivistettä. Jos tiivisteet täsmäävät, dataa ei ole muutettu allekirjoituksen jälkeen. [112]

Menetelmän luotettavuuden kannalta on ehdottoman tärkeää, että yksityinen avain on ja pysyy ainoastaan omistajansa hallussa.[113] Varmentamattomassa kehittyneessä sähköisessä allekirjoituksessa riskinä on, että omistajaa ei ole identifioitu avainpariin luotettavasti.

4.3 Varmennettu sähköinen allekirjoitus

Varmennettu sähköinen allekirjoitus on kehittynyt sähköinen allekirjoitus, joka perustuu hyväksyttyyn varmenteeseen ja on luotu turvallisella allekirjoituksen luomismenetelmällä.[114]

Sähköisistä allekirjoituksia koskevista puitteista direktiivin 2. artiklan mukaan kehittyneen sähköisen allekirjoituksen tulee täyttää seuraavat vaatimukset:

a. se liittyy yksiselitteisesti sen allekirjoittajaan
b. sillä voidaan yksilöidä allekirjoittaja
c. se on luotu keinolla, jotka allekirjoittaja voi pitää yksinomaisessa valvonnassaan; ja
d. se on liitetty sen kohteena olevaan tietoon siten, että tiedon mahdollinen myöhempi muuttaminen voidaan havaita

---

[112] Rinne 2002 s. 89.
[113] Liikenne- ja viestintäministeriö 2003 s. 27.
[114] KOM 2006/120/EY s. 4-5. Varmennetun sähköisen allekirjoituksen on täytettävä direktiiviin 1999/93/EY I, II ja III liitteissä asetetut vaatimukset.

Vaikka direktiivi on lähtökohtaisesti teknologianeutraali, käytännössä 2. artiklan mukaisilla vaatimuksilla tarkoitetaan luotettavasti varmennettua PKI-järjestelmään pohjautuvaa sähköistä allekirjoitusta. Varmennetun sähköisen allekirjoituksen tulee myös 5. artiklan mukaan täyttää sähköisessä muodossa olevan tiedon osalta allekirjoituksille asetettavat oikeudelliset edellytykset samalla tavoin kuin käsin kirjoitettu allekirjoitus täyttää kyseiset vaatimukset paperilla. Varmennetun sähköisen allekirjoituksen tulee myös kelvata todisteeksi oikeudellisissa menettelyissä.

Varmennetun sähköisen allekirjoituksen luotettavuus saavutetaan käyttämällä luotettuja kolmansia osapuolia varmentajina[115] (TTP, Trusted Third Parties). Esimerkiksi viranomaistaho toimii kolmantena osapuolena ja todentaa asioinnin osapuolet tai jonkun osapuolista. PKI-järjestelmässä kaikkien on luotettava TTP-osapuoleen, joka vastaa siitä, että varmenteet on jaettu todellisille omistajille ja että varmenteen tiedot ovat oikein.[116]

Suomessa viestintävirasto pitää rekisteriä hyväksytyistä laatuvarmennepalvelujen tarjoajista ja liikenne- ja viestintäministeriö huolehtii varmennetoiminnan yleisestä ohjauksesta ja kehittämisestä. Viestintäviraston tehtäviin kuuluu myös uusien laatuvarmennepalvelujen tarjoajien hakemuksien käsittely ja valvonta toiminnan lain-mukaisuudesta niin laatuvarmennepalvelujen tarjoajan oman tietoturvan, taloudellisen aseman kuin varmenteen sisältävien tietojen oikeellisuuden varmistamisenkin osalta. Laatuvarmennepalvelun tarjoajalla on vahingonkorvausvelvollisuus tilanteessa, jossa varmenteeseen merkityt tiedot osoittautuvat virheellisiksi tai lain määräyksiä jätetään noudattamatta.[117]

Direktiivin sähköisiä allekirjoituksia koskevista yhteisön puitteista liitteessä I on määritelty tarkemmin, mitä tietoja laatuvarmenteen tulee sisältää ja liitteessä II on lueteltu hyväksyttyjä varmenteita myöntävien varmennepalvelujen tarjoajia koskevat vaatimukset (tutkielman liite 1).

---

[115] Ainoana luotettuna kolmantena osapuolena toimii Suomessa väestörekisterikeskus, kansainvälisiä luotettuja kolmansia osapuolia ovat muun muassa Root CA, Bridge CA ja Bridge/Gateway CA.
[116] Rinne 2002 s. 91.
[117] Järvinen 2003 s. 171.

PKI-järjestelmällä tarkoitetaan varmenteiden myöntämisestä, jakelusta, hallinnoinnista ja ylläpidosta muodostuvaa kokonaisuutta. PKI-järjestelmä sisältää käytännössä aina tietyt peruspalvelut. Peruspalveluina voidaan pitää varmennetta hakevan tahon rekisteröintiä, varmenteiden luontia ja varmenteiden jakelua varmenteen hakijalle. PKI-järjestelmään kuuluu olennaisena osana ajan tasalla olevan varmennehakemiston sekä sulkulistan ylläpito. Varmennehakemistossa säilytetään kaikkia myönnettyjä varmenteita ja sulkulistalla ennen vanhentumistaan mitätöityjä varmenteita. Myös ylläpito- ja tukipalvelut sekä toimintakuvaus kuuluvat PKI-järjestelmän peruspalveluihin.[118]

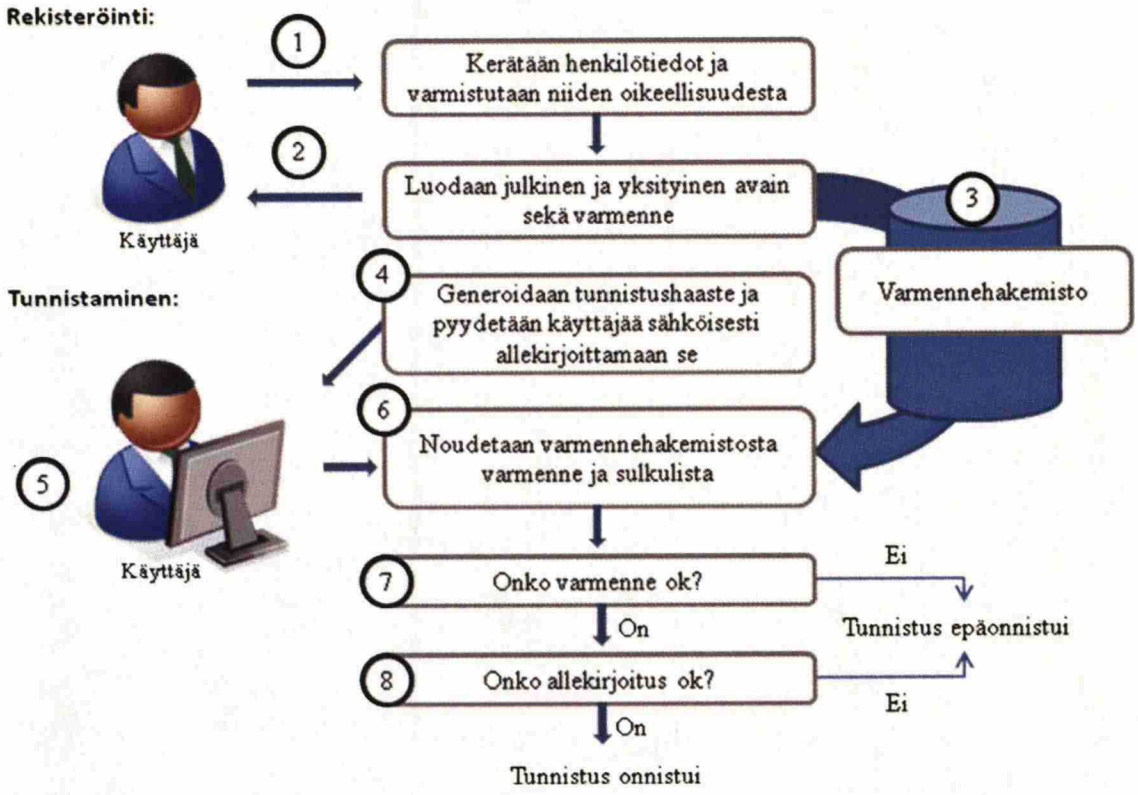
Laajat PKI-järjestelmät ovat rakenteeltaan hierarkkisia eli varmenteiden myöntäminen ei tapahdu keskitetysti vaan se on hajautettu lähemmäksi käyttäjiä. Myöntäjän sijainti lähellä varmennettavia parantaa tietoturvaa, koska silloin tietojen oikeellisuuden tarkistaminen ja varmenteiden turvallinen jakelu on helpompi toteuttaa.[119] PKI-järjestelmät voivat olla yhden yrityksen kattavia, maan tai ehkä tulevaisuudessa koko EU:n kattavia järjestelmiä.[120] Direktiivi sähköisiä allekirjoituksia koskevista yhteisön puitteista koskee yleisölle palvelujaan tarjoavia palveluntarjoajia, jättäen yritysten sisäiset PKI-järjestelmät lainsäädännön ulkopuolelle.[121]

Hierarkkinen PKI-järjestelmä perustuu juurivarmenteeseen, jolla allekirjoitetaan aina alemmantason varmenteet. Järjestelmän tietoturva pohjautuu juurivarmenteeseen, joten sen säilyminen turvallisena on edellytys koko PKI-järjestelmän uskottavuudelle.[122]

Ohessa kuvataan kaavioiden avulla varmennetun sähköisen allekirjoituksen rekisteröinti- ja tunnistusprosessi sekä allekirjoitusprosessi:

---

[118] Järvinen 2003 s. 166.
[119] Järvinen 2003 s. 168.
[120] Järvinen 2003 s. 165.
[121] Järvinen 2003 s. 171.
[122] Järvinen 2003 s. 170.



Kuvio 3: Varmenteisiin perustuva rekisteröinti- ja tunnistusprosessi[123]

Rekisteröinti:

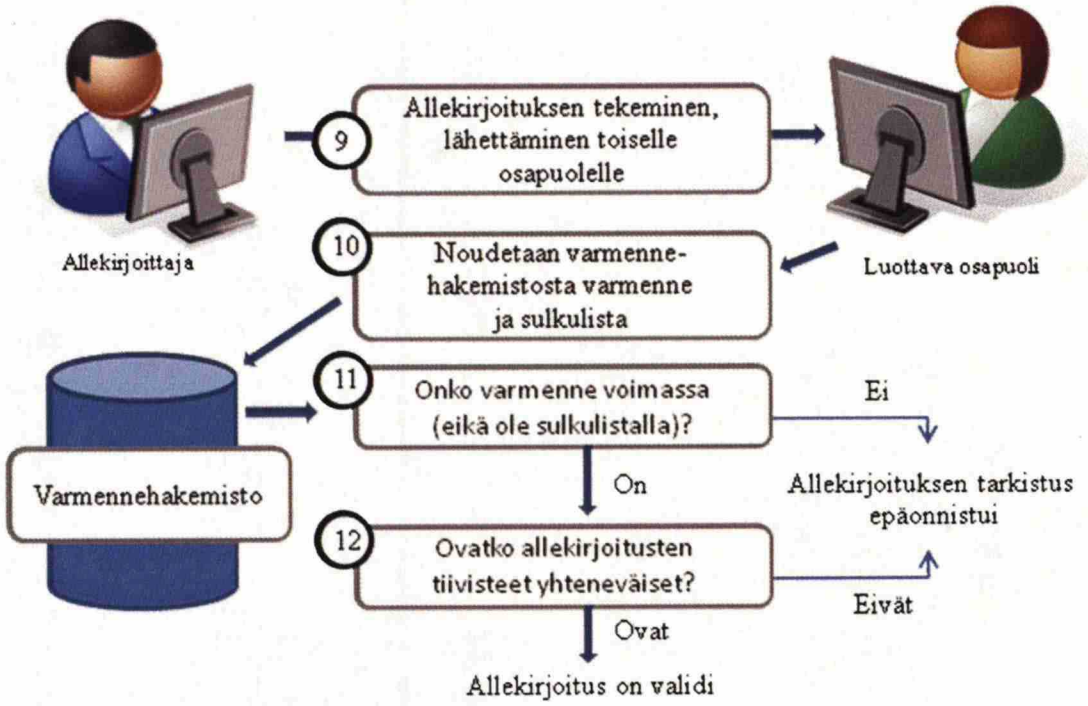
1. Rekisteröintipisteessä rekisteröijä varmistaa henkilön henkilöllisyyden hyväksyttävällä ja luotettavalla menetelmällä. Henkilöstä kerätään tarpeelliset henkilötiedot sekä mahdollisesti muuta lisätietoa.
2. Henkilölle generoidaan yksityinen ja julkinen avain. Yksityinen avain luovutetaan käyttäjälle (esim. älykortilla). Julkinen avain ja henkilötiedot tallennetaan varmenteeseen. Varmenteen myöntäjä allekirjoittaa sähköisesti varmenteen. Toimenpide varmistaa sen, että varmennetta ei ole myöntämisen jälkeen muutettu.[124] Käyttäjälle luovutetaan joko viittaus varmenteeseen tai itse varmenne.
3. Varmenne tallennetaan varmennehakemistoon.

---

[123] Liikenne ja viestintäministeriö 2003 s. 32–34 (mukaillen). Kaaviota on yksinkertaistettu alkuperäisestä liikenne ja viestintäministeriön selostuksesta, koska tarkoituksena on selkeyttää rekisteröinti- ja tunnistusprosessia kiinnittämättä liikaa huomiota teknisiin yksityiskohtiin. Vaihekohtaiseen selostukseen on lisätty kohtia selkeyttämään rekisteröinti- ja tunnistamisprosessia.
[124] Rinne 2002 s. 91.

Tunnistaminen:

4. Tunnistava taho generoi tunnistushaasteen, joka lähetetään tunnistettavalle henkilölle sähköisesti allekirjoitettavaksi. Tunnistushaasteen sisällöllä ei ole merkitystä, mutta tunnistushaasteen tulee olla jokaisella kerralla erilainen tietoturvasyistä.
5. Käyttäjä allekirjoittaa tunnistushaasteen omalla yksityisellä avaimellaan. Allekirjoitus ja käyttäjän varmenne tai viittaus varmenteeseen lähetetään tunnistavalle taholle.
6. Tunnistava taho noutaa varmennehakemistosta käyttäjän varmenteen, jos käyttäjä ei ole sitä allekirjoituksen yhteydessä itse toimittanut. Varmennehakemistosta noudetaan lisäksi sulkulista.
7. Tunnistava taho tarkistaa varmenteen voimassaolon ja muuttumattomuuden. Voimassaolo tarkistetaan voimassaolopäiväyksestä ja varmistamalla ettei varmenne ole sulkulistalla. Sulkulista sisältää kuoletetut varmenteet. Varmenteen muuttumattomuus tarkastetaan tarkastamalla varmenteen myöntäjän tekemä sähköinen allekirjoitus.
8. Tunnistava taho tarkastaa käyttäjän toimittaman tunnistehaasteen allekirjoituksen. Salattu tunnistushaaste eli allekirjoitus puretaan varmenteessa olevalla julkisella avaimella. Jos salauksen purun tuloksena saatu vastine on identtinen alkuperäisen kanssa, tunnistus hyväksytään.



Kuvio 4: Varmenteisiin perustuva allekirjoitusprosessi[125]

Allekirjoittaminen:

9. Allekirjoittava taho generoi allekirjoituksen ja lähettää sen ja käyttämänsä varmenteen varmenteeseen luottavalle osapuolelle. Allekirjoitus muodostetaan välitettävästä aineistosta lasketun tiivisteen avulla, joka allekirjoitetaan salaisella avaimella. Salattu tiiviste eli sähköinen allekirjoitus liitetään välitettävän aineiston mukaan.
10. Luottava osapuoli noutaa varmenteen sekä sulkulistan.
11. Luottava osapuoli tarkastaa varmenteen voimassaolon ja ettei sitä ole merkitty sulkulistalle. Varmenteen eheys tarkistetaan varmentajan sähköisestä allekirjoituksesta.
12. Luotettava osapuoli purkaa julkisella avaimella tiivisteen, laskee vastaanottamastaan aineistosta tiivisteen ja vertaa saamiaan tiivisteitä toisiinsa. Jos tiivisteet ovat identtisiä, allekirjoitus on validi.

---

[125] Liikenne ja viestintäministeriö 2005b s. 17.

Varmentaminen tunnistamis- ja allekirjoitustarkoituksiin ovat eri asioita. Kaupallisesti näitä tarjotaan yhdessä, mutta oikeudellisesti vain allekirjoitusvarmennetta tulee pitää laatuvarmenteena, koska lakia sähköisistä allekirjoituksista sovelletaan ainoastaan allekirjoitusvarmenteisiin. Tunnistautumis- ja allekirjoitusvarmenne ovat teknisesti hyvin samankaltaisia. Esimerkiksi väestörekisterikeskuksen HST-korttia käytettäessä tunnistamiseen ja allekirjoitukseen pätevät samat tietoturvatasot, mutta itse tunnistamis- ja allekirjoitusprosessissa käytetään eri PIN-lukuja.[126]

EU:n sisälle pyritään luomaan infrastruktuuri direktiivin avulla, jonka pohjalta toimiviin varmennepalvelujen tarjoajiin ja varmenteisiin jäsenmaat voisivat luottaa sekä luoda yhteisen käytännön varmenteiden ja niitä hyödyntävien palveluiden käyttämiseen.

4.3.1 Sähköisen allekirjoituksen luomisvälineet

Turvallisen allekirjoituksen luomismenetelmän (Secure Signature Creation Device) on täytettävä direktiivin sähköisiä allekirjoituksia koskevista yhteisön puitteista liitteessä III vahvistetut vaatimukset (tutkielman liite 1):

a. allekirjoituksen luomiseen käytettäviä tietoja voidaan käyttää vain kerran ja ne säilyvät luottamuksellisina
b. allekirjoituksen luomiseen käytettäviä tietoja ei voida johtaa muista tiedoista
c. allekirjoitus on suojattu väärentämiseltä
d. allekirjoittaja voi suojata allekirjoituksen luomiseen käytettävät tiedot muiden käytöltä

Allekirjoitusvälineen luomisvälineen tulee olla EU:n vahvistaman yleisesti tunnustetun standardin mukainen. Se voi olla myös Suomessa tai Euroopan talousalueeseen kuuluvassa valtiossa nimetyn tarkastuslaitoksen hyväksymä allekirjoituksen luomisväline.[127] Sähköisistä allekirjoituksista annetun lain (24.1.2003/14) 18§:ssä

---

[126] Liikenne- ja viestintäministeriö 2005b s. 18.
[127] Laki sähköisistä allekirjoituksista (24.1.2003/14) 6 §.

todetaan, että jos oikeustoimeen vaaditaan lain mukaan allekirjoitus, vaatimuksen täyttää ainakin sellainen kehittynyt sähköinen allekirjoitus, joka perustuu laatuvarmenteeseen ja on luotu turvallisella sähköisen allekirjoituksen luomisvälineellä.[128]

Sähköisen allekirjoituksen luomisvälineen määritelmää Suomen lainsäädännössä tulisi tarkentaa. Yksityisten henkilöiden ja eri toimijoiden on vaikea tämän hetken Suomen lainsäädännöstä ymmärtää, mitä sähköisen allekirjoituksen luomisvälineen määritelmään sisältyy. Tarkoitetaanko sähköisen allekirjoituksen luomisvälineellä esimerkiksi allekirjoituksen generoivaa laitetta vai tarvittavien ohjelmistojen ja ajurien kokonaisuutta? Yksityistä kuluttajaa taas kiinnostaa, mitkä tekniset laitteet tai laitekokonaisuudet ovat hyväksyttyjä ja testattuja.[129]

4.3.2 Varmennetun sähköisen allekirjoituksen riskit

Julkisen avaimen menetelmään perustuva varmennettu sähköinen allekirjoitus on erittäin luotettava, koska PKI-järjestelmän perustana olevat laskentamallit ja algoritmit on kehitetty jo vuosikymmeniä sitten, joten niiden turvallisuutta on voitu arvioida jo pitkään.[130] Kaikissa menetelmissä on kuitenkin riskinsä, ja varmennepohjaisissa menetelmissä riskit voidaan jakaa kortinhaltijan aiheuttamiin riskeihin, kortinlukijan, päätelaitteen sekä ohjelmiston turvallisuuden aiheuttamiin puutteisiin sekä kortin myöntäjään ja varmentajaan liittyviin riskeihin.[131]

Kortinhaltijan vaikutus älykortin turvallisuuteen on keskeisessä asemassa. Älykortin fyysinen turvallisuus ja yksityisen avaimen säilyminen vain käyttäjän hallussa ovat kortin turvallisen käytön edellytyksiä. Sirulliset älykortit ovat hyvin turvallisia, koska yksityinen avain ei poistu sirukortilta ollenkaan. Älykortin PIN-luvun pitäminen salassa

---

[128] Laine (toim.) 2001 s. 208.
[129] Liikenne- ja viestintäministeriö 2005 s. 10.
[130] Liikenne- ja viestintäministeriö 2003 s. 41.
[131] Rinne 2002 s. 65–73.

on kortin haltijan tärkein turvatoimenpide. PIN-lukua ei saisi kirjoittaa ylös, se ei saa olla liian helppo, eikä sitä missään nimessä saa säilyttää kortin yhteydessä.[132]

Kortinlukijan ja päätelaitteen turvallisuudesta aiheutuvat puutteet voidaan nähdä myös tietoturvariskinä. Riskin voi muodostaa kortinlukijalaite tai esimerkiksi haittaohjelmisto, joka voi mahdollisesti tallentaa PIN-luvun ja muuta luottamuksellista tietoa. Suurin osa tietokoneista on yhteydessä Internetiin, joten huonosti suojattuun koneeseen ulkopuolinen taho voi onnistua asentamaan haittaohjelman käyttäjän sitä huomaamatta.[133] Riski liittyy siis siihen, että voidaanko olla varmoja, ettei lukijalaite tai jokin ohjelmisto tallenna PIN-lukua.[134]

Teoriassa sekä kortin että varmenteiden myöntäjään liittyy myös tietoturvariski. Turvallisuuden kannalta on olennaista kyetä tunnistamaan älykortin haltija ja se että älykortti luovutetaan oikealle haltijalleen. Itse älykortin valmistuksen yhteydessä tulee varmistua, että alihankkijat myös noudattavat turvallisuusvaatimuksia.[135] Luottamus itse varmenteen myöntäjään on varmennepohjaisissa menetelmissä ensiarvoisen tärkeää. Varmentajan tulee myös ylläpitää ajantasaista ja täsmällistä sulkulistapalvelua luottamuksen säilyttämiseksi.[136] Suomessa kansalaisvarmenteen myöntäjän Väestörekisterikeskuksen luotettavuus lienee itsestään selvä, mutta laajoihin rekistereihin liittyy aina riskinsä.[137]

Esimerkiksi Englannissa 25 miljoonan ihmisen henkilö- ja pankkitiedot[138] sekä 160 000 lapsen nimi ja osoitetiedot[139] onnistuttiin hukkaamaan tietoturvaproseduurien laiminlyömisen vuoksi vuonna 2007. Vuonna 2008 Englannissa varastettiin Kuninkaallisen Laivaston upseerin kannettava tietokone, jossa säilytettiin laivaston

---

[132] Rinne 2002 s. 67–68.
[133] Rinne 2002 s. 70.
[134] Liikenne- ja viestintäministeriö 2003 s. 38.
[135] Rinne 2002 s. 71.
[136] Liikenne- ja viestintäministeriö 2003 s. 41.
[137] Liikenne- ja viestintäministeriö 2005a s. 38 ja viestintäviraston määräys 7/2003. Laatuvarmenteen Suomessa voi myöntää sähköisistä allekirjoituksista säädetyssä laissa säädetyt 10 § - 15 § vaatimukset täyttävä varmentaja.
[138] BBC News 2007. Ks. http://news.bbc.co.uk/go/pr/fr/-/1/hi/uk_politics/7103566.stm.
[139] Australian IT 2007. Ks. http://www.australianit.news.com.au/story/0,24897,22968521-15306,00.html.

600 000 nimeä kattavaa rekisteriä.[140] Englannissa onkin spekuloitu, onko kansalaisten luottamuksen palauttaminen valtionhallintoon uuden sähköisen henkilökortin rekisterin ylläpitäjänä enää mahdollista.

4.3.3 Väestörekisterikeskuksen kansalaisvarmenne HST-kortti

Väestörekisterikeskuksen yksityishenkilöille 1.4.2003 alkaen myöntämä kansalaisvarmenne on ainoa laatuvarmenne Suomessa joka täyttää kaikki sähköisiä allekirjoituksia koskevan lain ja direktiivin asettamat kriteerit varmennetulle sähköiselle allekirjoitukselle.[141] HST-korttien (henkilön sähköinen tunnistaminen[142]) myöntäminen aloitettiin 1.12.1999, mutta vasta eduskunnan hyväksyttyä lain sähköisistä allekirjoituksista ja lain sähköisestä asioinnista viranomaistoiminnassa HST-kortilla tehdyt allekirjoitukset tulivat yhdenveroisiksi perinteisten allekirjoitusten kanssa.

HST-kortin päätavoite on mahdollistaa henkilöllisyyden todistaminen verkkopalveluissa sekä tekstien ja tiedostojen sähköinen allekirjoittaminen eli oikeustoimien tekeminen sähköisesti. Lisäksi itse kortti toimii passin korvaavana matkustusasiakirjana tällä hetkellä EU-maissa ja eräissä muissa maissa.[143] Henkilökorttilain (300/2003) uudistuksen yhteydessä vanhan siruttoman henkilökortin myöntäminen lopetettiin.

Väestörekisterikeskuksen HST-kortin varmennehierarkia koostuu kolmesta eri varmenteesta. Ylimmällä tasolla on Väestörekisterikeskuksen juurivarmenne, toisella tasolla on kansalaisvarmenteisiin käytettävä varmenne ja alimpana henkilölle myönnetty kansalaisvarmenne. Jokainen varmenne on allekirjoitettu sähköisesti ylemmän tason varmenteella. Kuten edellä mainittiin, on juurivarmenteen turvallisena säilyminen edellytys koko PKI-järjestelmän uskottavuudelle. Väestörekisterikeskuksen HST-järjestelmässä juurivarmenne on 2048-bittinen, kun tavalliset kansalaisvarmenteet ovat 1024-bittisiä. Kaikki tiedot missä ja miten juurivarmenteen yksityistä avainta säilytetään on luokiteltu salaisiksi.

---

[140] The Times 2008. Ks. http://www.timesonline.co.uk/tol/news/politics/article3213274.ece.
[141] Männikkö 2007 s. 16.
[142] FINEID (The Finnish Electronic Identification).
[143] Järvinen 2003 s. 194. HST- kortti käy matkustusasiakirjana Liechtensteinissa, Sveitsissä ja San Marinossa.

Väestörekisterikeskuksen juurivarmenne on myös lisätty Microsoftin Windows-käyttöjärjestelmien päivitettyihin selainversioihin 27.6.2007 luotettujen varmenteiden listalle. Käyttäjien aiemmin saamat suojausvaroitukset varmenteesta poistuvat. Uudistuksen ansiosta sähköisten palveluiden käyttö Windows-käyttöjärjestelmissä nopeutuu ja helpottuu.[144]

HST-kortin käyttö omassa tietokoneessa edellyttää lukulaitetta (kuva 1) ja sopivaa ohjelmistoa. Koneeseen kortinlukijan voi kytkeä monella eri tavalla, esimerkiksi sarjaporttiin, PC-Card-paikkaan tai USB-porttiin. Kun lukijalaite on asennettu, kortti aktivoituu heti lukijan laitettaessa. Kirjauduttaessa HST-korttia tukevaan palveluun, ei tarvita lukijalaitteen ja kortin lisäksi kuin PIN-luku.[145]

Kuva 1: Älykortinlukija SCR3310 (valmistaja SCM Microsystems Inc, yhteensopiva HST-kortin kanssa) sekä väestörekisterikeskuksen HST-kortti.

Tilanne jossa HST-korttia käytetään oikeustoimen tekemiseen, kuten esimerkiksi sopimuksen tai kauppakirjan hyväksymiseen allekirjoitetaan sähköinen asiakirja syöttämällä ensin PIN-luku ja sen jälkeen vielä PIN2-luku, jolla vahvistetaan tehtävä oikeustoimi. PIN-luku on tunnistamista ja salausta varten ja PIN2-luku on varsinaista sähköistä allekirjoitusta varten. Jos PIN-luku syötetään väärin kolme kertaa peräkkäin, kortti lukkiutuu.[146] Lukkiutuneen kortin voi avata vain poliisilaitoksella, jossa kortti avataan. Fyysisesti HST-kortin lukeminen esimerkiksi elektronisella mikroskoopilla tai

---

[144] Katso www.etu-klubi.fi / Väestörekisterikeskus luotettava varmentaja Microsoft Windows-käyttöjärjestelmässä, 4.2.2008.
[145] Järvinen 2003 s. 197–206.
[146] Järvinen 2003 s. 206–209.

mittapäällä on mahdotonta, myöskään kortin uudelleen ohjelmointi ei ole mahdollista.[147]

4.4 Sähköisen allekirjoituksen nykytila Suomessa

Yleisimmät Suomessa käytössä olevat sähköisten allekirjoitusten sovellukset liittyvät sähköiseen hallintoon tai henkilökohtaisiin pankkipalveluihin. Sähköisen hallinnoinnin palveluissa voi tällä hetkellä käyttää HST-korttia tai vaihtoehtoisesti TUPAS-pankkitunnisteita. Monet EU-jäsenvaltiot ovat myös ottaneet tai aikovat ottaa käyttöönsä sähköiseen allekirjoitukseen perustuvia sähköisen hallinnon sovelluksia.[148] Tällä hetkellä pankkipalveluissa käytetään käytännössä eri pankkien TUPAS-pankkitunnusteita, ainoana poikkeuksena Osuuspankki, jossa on mahdollista myös käyttää HST-korttia. Verkkokaupoissa ei käytännössä käytetä varmennettua sähköistä allekirjoitusta vaan sopimus tehdään käyttäen sähköistä allekirjoitusta laajassa mielessä.

HST-kortin ongelmaksi Suomessa on muodostunut vähäinen palvelutarjonta. Tällä hetkellä HST-kortin tunnistautumista hyödyntäviä palveluja on noin 60, joista suurin osa on valtionhallinnon palveluita.[149] Uusien palvelujen markkinoille tuloa edistääkseen väestörekisterikeskus alkoi jakaa avoimen lähdekoodin ohjelmaa, jonka avulla HST-kortin tuen lisääminen elinkeinonharjoittajien palvelusovelluksiin helpottui.[150]

Myöskään selkeiden ja yksinkertaisten käyttöliittymien suunnittelussa ei ole vielä täysin onnistuttu allekirjoitusvälineiden ja ohjelmistojen suhteen. Palveluiden käyttäjät eivät välttämättä ole tietoisia hetkestä jolloin sähköinen allekirjoitus generoidaan. Generointihetkellä sopimus astuu voimaan. Perusedellytyksenä oikeusvaikutuksille on kuitenkin se että tahdonilmaisu on harkittu. Allekirjoitusvälineiden ja ohjelmistojen

---

[147] Moilanen – Pellinen – Romanainen 2002 s. 16.
[148] KOM 2003/567/EY s. 8–9.
[149] Kuluttajatutkimuskeskus 2007 s. 13.
[150] Ks. http://www.vaestorekisterikeskus.fi/vrk/bulletin.nsf/vwSearchView/ EA405E8936FF1155C22 56D0A002BAF31

käyttöliittymille tulisi määritellä yksiselitteisiä ohjeistuksia, käytäntöjä ja tarkastusmenettelyjä.[151]

HST-kortin uskottavuuden ongelmista kertoo myös se, että henkilökohtaisissa pankkipalveluissa[152] käytetään todentamiseen edelleen kertakäyttöisiä salasanoja ja varmistustunnuksia (TUPAS-pankkitunnisteita) eli direktiivin mukaan kyseessä on yksinkertaisin sähköisen allekirjoituksen muoto. Monissa pankkipalveluissa näitä tekniikoita käytetään vain käyttäjän henkilöllisyyden todentamiseen, mutta myös sähköinen maksumääräysten allekirjoittaminen on lisääntymään päin. Yritysten välisessä ja pankkien välisessä maksuliikenteessä on yleisempää käyttää älykortteja, joiden katsotaan tarjoavan korkeamman tietoturvatason.[153]

Väestörekisterikeskuksen yksityishenkilöille myöntämän kansalaisvarmenteen on hankkinut vasta vajaat 152 300[154] suomalaista kun taas TUPAS-pankkitunnisteita on noin 3,6 miljoonaalla suomalaisella.[155] Esimerkiksi Virossa noin 700 000 kansalaisella on sähköinen henkilökortti ja tarjolla on noin 150 sähköistä palvelua. Kuitenkin vain 3 % virolaisista käyttää sähköisissä palveluissa sähköistä henkilökorttia pankkitunnisteiden sijaan.[156]

4.5 Sähköinen allekirjoitus tulevaisuudessa

Varmennetun sähköisen allekirjoituksen ja kertakäyttöisten tunnuslukujen heikoimpana kohtana voidaan pitää henkilökohtaista PIN-lukua tai asiakasnumeroa. Tunnuksensa muille luovuttava asiakas on kummankin järjestelmän suurin epävarmuustekijä. Vihamielinen taho voi myös pakottaa kortin haltijan kertomaan PIN-lukunsa.[157] Varmenteeseen pohjautuvan älykorttipohjaisen sähköisen allekirjoituksen luotettavuutta

---

[151] Liikenne- ja viestintäministeriö 2005a s. 8.
[152] HST-kortilla on mahdollista ainoastaan käyttää Osuuspankin verkkopankkipalvelua.
[153] KOM 2006/120/EY s. 6.
[154] HST-korttia on myönnetty 31.12.2007 mennessä 169 400:lle henkilölle, joista voimassaolevia 152 300 kpl. (Ks. http://www.sahkoinenhenkilokortti.fi/vrk/bulletin.nsf/HeadlinesFineid/9FFCB6B94B153AA9C22573CC004D5C84, 1.2.2008).
[155] Männikkö 2007 s. 13.
[156] Liikenne- ja viestintäministeriö 2005b s. 40.
[157] Rinne 2002 s. 68.

voitaisiin tulevaisuudessa parantaa tunnistamalla kortinhaltija biometrisellä tunnisteella, esimerkiksi sormenjäljen tai verkkokalvon perusteella.[158]

Biometrisissä tunnistusmenetelmissä henkilöstä mitataan jokin henkilön muuttumaton fyysinen ominaisuus, kuten sormenjälki, kämmenen rakenne, kasvot tai silmän iiris. Tunnistustilanteessa ominaisuutta verrataan tietovarastossa olevaan tallennettuun ominaisuuteen. Jos tietovarastosta löytyy yhtenevä tallenne, voidaan tunniste sen perusteella yhdistää henkilötietoihin.[159]

Biometrisen tunnisteen vahvuutena voidaan pitää erittäin vaikeata väärennettävyyttä. Henkilö ei voisi edes antaa tunnistetta eteenpäin, koska toisella henkilöllä ei ole hänen sormenjälkeäkään. Biometrisen tunnisteen heikkoutena voidaan pitää todennäköisyyksien vaikutusta tunnistusprosessiin. Muissa menetelmissä tulos on joko että henkilö on tai ei ole kuka hän väittää olevansa. Biometrisen tunnisteen todentamisessa henkilö on tai ei ole tietyllä todennäköisyydellä väittämänsä henkilö. Biometrisen tunnistusjärjestelmän tulisi myös pystyä tarkistamaan, että sormenjälki tulee esimerkiksi aidosta ja elävästä sormesta.[160]

Ihmisen fyysisiin ominaisuuksiin perustuvaan biometriseen tunnistamiseen tarvittava tekniikka on jo olemassa, mutta käytännön sovellukset ovat vielä harvassa. Biometrinen tunnistaminen vaatii lukijalaitteiden hankkimista ja asentamista. Uusista kannettavista osasta löytyy jo esimerkiksi sormenjälkitunnistin vakiovarusteena. Sovelluksia biometrisestä tunnistamisesta on myös otettu arkipäiväiseen käyttöön, kuten esimerkiksi tietyillä kuntosaleilla sormenjälkitunnistukseen perustuvat tunnistusjärjestelmät.

Biometristen tietojen säilyttäminen yhdessä henkilötietojen kanssa on kuitenkin ongelmallista koska jos tiedot päätyvät vääriin käsiin, on biometrisen ominaisuuden, kuten esimerkiksi sormenjäljen, kuolettaminen mahdotonta. Myös biometriset tunnistusmenetelmät jotka mahdollistavat yksilön automaattisen tunnistamisen esimerkiksi liikeratojen tai äänen koostumuksen mukaan luovat riskin yksilön

---

[158] Liikenne- ja viestintäministeriö 2003 s. 43.
[159] Liikenne- ja viestintäministeriö 2003 s. 31.
[160] Liikenne- ja viestintäministeriö 2003 s. 42.

anonymiteetille.[161] Biometristen tietojen tallentamiseen suhtaudutaankin varsin kriittisesti. Riskinä on tallenteiden ei-hyväksyttävä kopioiminen ja levittäminen.

Biometristen tietojen muodostamisesta, käsittelystä ja tallentamisesta tulisi säätää lainsäädännössä, koska biometriset ominaisuudet ovat pysyvä osa henkilöä. Oikeudellisten sääntelyn tarvetta lisää se, että tiettyjen biometristen ominaisuuksien tunnistaminen etälukemalla on mahdollista, ilman että henkilö tiedostaa sen. Sääntelyn avulla voitaisiin turvata yksityiselämän suoja ja yksilön oikeudet sekä kaupallisten palveluiden toimivuuden ja tasavertaisuuden turvaaminen. Toistaiseksi lainsäädännössä ei ole suoraan biometrisiä tietoja koskevia säännöksiä, mutta nykyisen henkilötietolain voidaan katsoa sääntelevän jo nykyisellään henkilön biometrisiä tietoja. Henkilön yksilöivä biometrinen ominaisuus on henkilötietolain mukainen henkilötieto ja henkilön tunnistamisessa tarvittava vertailurekisteri on henkilötietolain mukainen henkilörekisteri.[162]

---

[161] Kuluttajatutkimuskeskus 2007 s. 6.
[162] Liikenne- ja viestintäministeriö 2003 s. 55–56.

5. Sähköisen asiakirjan todentaminen

Sähköisen sopimuksen muodollisesta pätevyydestä riippumatta merkitystä on sillä, kuinka sähköisen asiakirjan sisällön voi tarvittaessa näyttää toteen. Perinteisellä paperiasiakirjalla ja sen allekirjoittamisella voidaan varmistua siitä, että sopijapuolet voivat tarvittaessa todistaa sopimussidonnaisuuden sisällön ja identifioida sopimuksen osapuolet.[163] Esimerkiksi tavallisen sähköpostin väärentäminen, samoin kuin useimpien sähköisten asiakirjamuotojen muuttaminen niin, että sitä on jälkikäteen vaikea huomata, on käytännössä helppoa.[164] Esimerkiksi, jos sekä elinkeinonharjoittaja että kuluttaja riitatilanteessa tarjoavat omaa versiotaan sopimusehdoista, voi käytännössä olla hyvinkin hankala osoittaa, mitkä ehdot asiakas todella sai tai mitkä ehdot olivat verkkokaupassa esillä. Toisaalta paperiasiakirja ei ole juurikaan turvallisempi. Paperiasiakirjan vahvuus todisteena selittyykin paljolti sillä, että se käytännössä kiistetään kohtuullisen harvoin.

Sähköisen asiakirjan todentaminen pitää sisällään tiedon alkuperän todentamisen, tiedon eheyden ja sen kiistämättömyyden. Jotta oikeustoimia voitaisiin tehdä luotettavasti sähköisesti, täytyy niille löytää sähköiset vastineet.[165]

---

[163] KOM 1990:20 s. 57–58.
[164] Laine (toim.) 2001 s. 205.
[165] Laine (toim.) 2001 s. 212.

Taulukko 1: Omakätisen allekirjoituksen ja sähköisen allekirjoituksen todentamisvaatimukset[166]

	Omakätinen allekirjoitus	Sähköinen allekirjoitus
Tiedon alkuperän tunnistaminen	Kyllä	Kyllä
Kiistämättömyys	Kyllä	Kyllä
Eheys	Kyllä	Kyllä
Linkki sisältöön	Kyllä	Kyllä
Helppo todentaa	Kyllä	Kyllä
Vaikea väärentää	Ei	Kyllä
Todennettavissa niin kauan kuin oikeustoimella merkitystä	Kyllä	Kyllä (kustannuksia)
Allekirjoittajan identifiointi	Kyllä	Kyllä

Tiedon alkuperän todentamisen avulla allekirjoitus voidaan liittää yksiselitteisesti sen tekijään. Sähköistä allekirjoitusta voidaan käyttää omakätisen allekirjoituksen asemasta kunhan sähköisen allekirjoituksen ominaisuudet täyttävät vähintään samat toiminnalliset vaatimukset kuin omakätinen allekirjoitus. Julkisen avaimen menetelmällä tehdyllä sähköisellä allekirjoituksella asiakirjan todistusfunktio voidaan teoreettisesti jopa turvata perinteisiä paperiasiakirjoja korkeammalla varmuusasteella.[167] Pakottavat muotosäännökset saattavat kuitenkin estää tämän.

Asiakirjan eheydellä varmistutaan, että mikäli tietoa muutetaan asiakirjan hyväksymisen jälkeen, se on havaittavissa. Omakätisesti allekirjoitetussa asiakirjassa tiedon eheyttä pyritään varmistamaan allekirjoittamalla viimeinen sivu.[168] Sähköisen asiakirjan tietosisällön eheys voidaan todentaa luotettavasti sähköisellä allekirjoituksella. Eheydellä tarkoitetaan sisällön muuttumattomuutta sen luomisen jälkeen.[169] Jos

---

[166] Laine (toim.) 2001 s. 204–205 ja 212–213.
[167] Nurmi 1997 s. 101–103.
[168] Laine (toim.) 2001 s. 202.
[169] Rinne 1997 s. 60.

tietosisältö on muuttunut, viestistä lasketut tiivisteet eivät vastaa toisiaan. Ei ole myöskään mahdollista, että osa asiakirjasta olisi muuttunut, koska sähköinen allekirjoitus riippuu koko asiakirjasta. [170] Sähköinen allekirjoitus ei siis salaa kohteena olevaa asiakirjaa, vaan suojaa sen eheyden.[171]

Kiistämättömyys merkitsee henkilön sitoutumista tekemäänsä transaktioon niin, ettei sitä voida enää kieltää jälkikäteen. Omakätinen allekirjoitus luo oletuksen oikeustoimen tekijästä eli viestin lähettäjä tai vastaanottaja ei pysty kiistämään allekirjoitusta. On mahdollista, ettei omakätisellä tai sähköisellä allekirjoituksella oikeustoimen tehnyt henkilö ole tehnyt oikeustointa.[172] Verkossa tapahtuvaan henkilön identifiointiin liittyy useita ongelmia. Yleensä päätelaite voidaan yksilöidä esimerkiksi Internet Protocol -osoitteen (IP) avulla. Ongelma syntyy siis lähinnä sopimuksen tehneen luonnollisen henkilön, ei niinkään päätelaitteen tunnistamisesta.

Tiedon turvallisen todentamiseen tarvittavilta välineiltä voidaan vaatia tiettyjä ominaisuuksia, kuten linkkiä oikeustoimen sisältöön, helppoa todennettavuutta ja vaikeaa väärennettävyyttä sekä sitä, että ne ovat todennettavissa niin kauan kuin oikeustoimella on oikeudellista merkitystä.[173]

Omakätisesti allekirjoitetussa asiakirjassa linkki oikeustoimen sisältöön tapahtuu allekirjoittamalla asiakirja kun taas sähköisesti allekirjoitetussa asiakirjassa linkki siihen varmistuu asiakirjasta lasketun tiivisteen avulla.[174]

Todentamiseen käytettävän välineen tulee olla vaikea väärentää ja helppo todentaa. Sähköisesti tehdyn allekirjoituksen väärentäminen on käytännössä teknisesti mahdotonta, kun taas omakätisesti tehdyn suhteellisen helppoa. Myös käsin allekirjoitetun monisivuisen asiakirjan väärentäminen on mahdollista, koska välillä vain viimeinen sivu allekirjoitetaan, jolloin muut sivut on mahdollista vaihtaa ilman, että

---

[170] Laine (toim.) 2001 s. 210.
[171] Rinne 2002 s. 89.
[172] Laine (toim.) 2001 s. 202.
[173] Laine (toim.) 2001 s. 237.
[174] Laine (toim.) 2001 s. 212.

lukija havaitsee asiakirjan muuttuneen. Sähköisesti allekirjoitetussa monisivuisten asiakirjojen eheys ja linkki asiakirjaan varmistuu.[175]

Asiakirjan todentamisen tulisi olla mahdollista niin kauan kuin oikeustoimella on merkitystä. Omakätisesti allekirjoitetussa asiakirjassa allekirjoitus on todennettavissa niin kauan kuin asiakirja on olemassa.[176] Sähköinen asiakirja on todennettavissa niin kauan kuin julkinen avain on käytettävissä. Tämän vuoksi tulisi olla säännöksiä, kuinka kauan varmentajat ovat velvollisia huolehtimana julkisen avaimen säilyttämisestä.[177]

Perinteisen paperiasiakirjan ominaisuuksiin kuuluu myös ainutkertaisuus, edellyttäen että asiakirja on luotu yhtenä kappaleena. Alkuperäiseen asiakirjaan kytkettyjen oikeuksien käyttäminen muodostuu sähköisen asiakirjan kannalta ongelmaksi.[178] Ainutkertaisuuden merkitys korostuu esimerkiksi asiakirjan siirtofunktion yhteydessä, asiakirjan ollessa arvopaperi. Esimerkiksi arvo-osuusjärjestelmän käyttöönoton yhteydessä ongelma ratkaistiin siten, että palvelurekisterin kirjausmenettelyllä korvattiin perinteisen paperiasiakirjan funktio.[179]

Paperiasiakirjan alkuperäisyyden ja hallinnan funktiot voidaan siis saavuttaa sähköistä asiakirjaa käyttämällä korvaamalla perinteinen omakätinen allekirjoitus luotettavaan varmentajaan tukeutuvan julkisen avaimen menetelmään perustuvalla sähköisellä allekirjoituksella.[180] Julkisen avaimen menetelmään perustuva luotettavan varmentajan varmentama sähköinen allekirjoitus täyttää siis kaikki taulukossa 1 turvalliselta todentamisen välineeltä edellytetyt vaatimukset. [181]

---

[175]
[176] Laine (toim.) 2001 s. 204.
[177] Laine (toim.) 2001 s. 212.
[178] KOM 1990:20 s. 69.
[179] Nurmi 1997 s. 104.
[180] Nurmi 1997 s. 103–105 ja KOM 1990:20 s. 61. Esimerkiksi arvo-osuusjärjestelmän palvelurekisteri.
[181] Laine (toim.) 2001 s. 213.

5.1 Aikaleimapalvelut

Aikaleiman luonti- ja verifiointipalveluita voidaan hyödyntää esimerkiksi sähköisessä asiakirjassa tilanteessa, jossa jollekin oikeudelliselle toimenpiteelle on asetettu aikaraja tai jos oikeustoimen tekemisen ajankohtaan liittyy oikeusvaikutuksia.[182] Aikaleiman avulla voidaan myös todentaa sähköisen asiakirjan allekirjoittamisajankohta. Tilanteessa, jossa sähköinen allekirjoitus joutuu sulkulistalle, pystytään todistamaan asiakirjan olevan lainvoimainen näyttämällä toteen sen olevan allekirjoitettu ennen varmenteen joutumista sulkulistalle. Aikaleima mahdollistaa asiakirjojen pitämisen lainvoimaisina myös varmenteen vanhentumisen jälkeen mahdollistaen esimerkiksi sähköisten sopimusten pitkäaikaisen arkistoinnin.[183]

Aikaleimalla tarkoitetaan PKI-pohjaista sähköistä allekirjoitusta, joka sisältää viittauksen kohteena olevan tiedoston tiivistelukuun, sekä päivämäärän ja kellonajan. Aikaleimalla voidaan osoittaa tapahtuman tai toimenpiteen täsmällinen tapahtumahetki. Aikaleimaa ei liitetä sähköiseen asiakirjaan sen luomisen yhteydessä, vaan vasta jälkikäteen, joten siitä ei välttämättä voi johtaa asiakirjan tekohetkeä. Aikaleiman olennaisia piirteitä ovat kiistämättömyys ja molempien osapuolten luottamus aikaleimavarmentajaan, joka saavutetaan käyttämällä luotettua kolmatta osapuolta.[184]

Aikaleimapalveluiden tarjoajiin sovelletaan varmennepalveluiden tarjoajia koskevia yhteisötason säännöksiä[185]. Kansallista sääntelyä itse aikaleiman määritelmästä tai vaatimuksista ei Suomen lainsäädännössä ole. Aikaleimojen sääntelyä kansallisella tasolla on toivottu Väestörekisterikeskuksen ja eräiden yksityisten toimijoiden puolesta kun taas Viestintävirasto on kyseenalaistanut tarpeen sääntelyyn. Aikaleimapalvelujen sääntelykysymys on ongelmallinen, koska palvelut eivät ole teknisesti ja kaupallisesti kovinkaan kehittyneitä, mutta toisaalta aikaleimoja on jo säännelty kansallisessa lainsäädännössä esimerkiksi Saksassa, Italiassa ja Virossa. Kysymys onkin siitä,

---

[182] Liikenne- ja viestintäministeriö 2005b s. 56.
[183] Valtiovarainministeriö 2001 s. 9.
[184] Valtiovarainministeriö 2001 s. 1 ja 8.
[185] Sähköisiä allekirjoituksia koskevan direktiivin artiklassa 2(11) määritellään laaja varmennepalvelujen tarjoaja. Tämän laajan määritelmän mukaan aikaleimapalveluiden tarjoajat ovat samojen säännösten alaisia kuin varmennepalvelujen tarjoajat.

halutaanko aikaleimapalvelut toteuttaa ei-säännellyillä todistusharkintaan perustuvilla tavoilla vai uusilla kansallisilla oikeudellisilla säädöksillä.[186]

Hallinnollisesti ei ole päätetty kuka vastaisi julkishallinnon aikaleimapalvelun tuottamisesta, mutta Väestörekisterikeskuksen varmennepalveluiden myyntipäällikön Ari Häklin mukaan Väestörekisterikeskukselta löytyy tekniset valmiudet aikaleimapalvelujen tarjoamisen aloittamiseen tarvittaessa heti.[187] Varmaa on kuitenkin se, että sähköisten oikeustoimien lisääntyessä aikaleimojen käyttöä oikeustoimien todentamisessa tullaan hyödyntämään, jolloin todennäköisesti olisi tarpeellista määritellä aikaleima ja perusvaatimukset kansalliseen lainsäädäntöön.[188]

5.2 Sähköisen asiakirjan arkistointi

Tietoyhteiskunnassa sähköisiä asiakirjoja ja allekirjoituksia tulee olla mahdollista arkistoida luotettavasti, jotta niihin liittyvät oikeustoimet ovat todennettavissa niin kauan kuin niillä on merkitystä. EU:n sähköisen kaupan direktiivin mukaan jäsenmaiden on huolehdittava siitä että sopimuksen tekemiselle sähköisessä muodossa ei ole sopimusoikeudellisia esteitä, joten myöskään asiakirjan sähköiselle arkistoinnille ei saa olla oikeudellisia esteitä.[189]

Kirjallisuudessa arkistointiprosessikuvauksissa sähköinen allekirjoitus ja asiakirjan tietosisältö tulisi yhdistää niiden keskinäisen yhteyden todentamiseksi. Yhdistämisestä muodostettu tiiviste tallennettaisiin luotettavan kolmannen tahon tietojärjestelmään, joka aikaleimaisi tiivisteen. Aikaleima tulisi liittää asiakirjaan, sekä sähköisten allekirjoitusten osalta myös allekirjoituksen tekemisaika tulisi arkistoida.[190]

---

[186] Liikenne- ja viestintäministeriö 2005b s. 58–59.
[187] Puhelinkeskustelu Väestörekisterikeskuksen myyntipäällikkö Ari Häklin kanssa (25.2.2008).
[188] Liikenne- ja viestintäministeriö 2005b s. 59–60.
[189] Dumortier – Van den Eynde 2002 s. 1.
[190] Liikenne- ja viestintäministeriö 2005b s. 61. Ks. Dumortier & Van den Eynde 2002 sekä Euroopan Komissiolle tehty tutkimus The Legal and Market Aspects of Electronic Signatures (Dumortier, Kelm, Nilsson, Skouma ja Van Eecke).

Yhteisö- ja kansallisen tason lainsäädännössä ei ole erityisiä säädöksiä koskien sähköisten asiakirjojen luotettavaa arkistointia. Varsinaista tarvetta lakimuutoksiin kansallisessa lainsäädännössä ei ole, koska julkisella puolella arkistointilaitoksen norminantovaltuudet ovat ennestään riittäviä ja yksityisellä puolella sähköisille arkistointipalveluille ei ole kysyntää korkeiden kustannusten takia. Tällä hetkellä sähköiset arkistointipalvelut eivät ole kilpailukykyisiä yksityisellä puolella esimerkiksi tilitoimistojen arkistointipalveluiden kanssa. Alan kirjallisuudessa on ehdotettu että luotetuille arkistointipalveluille tulisi luoda oikeudellinen järjestelmä (Trusted Archival Service), joka tukeutuisi yhteisölainsäädäntöön.[191]

[191] Liikenne- ja viestintäministeriö 2005b s. 61.

6. Sähköisen sopimuksen muotovaatimukset

Muotovaatimuksella tarkoitetaan sopimuksen päättämiseen liittyviä seikkoja, joita edellytetään osapuolten tahdonilmaisujen lisäksi sopimuksen pätevyyden syntymiseksi.[192] Sähköiset sopimukset ovat sopimuksia, joissa ei ole mahdollista käyttää perinteistä kirjallista muotoa tai omakätistä allekirjoitusta. Verkkosopimuksille on kuitenkin ominaista, että tahdonilmaisujen vaihto tapahtuu tietoverkon välityksellä. Oikeustoimien tekeminen luotettavasti edellyttää sitä, että niiden tekijä voidaan tunnistaa ja sisältö luotettavasti varmistaa. Jos oikeustoimi on tehty kirjallisesti ja allekirjoitettu omakätisesti, voidaan sen tekijä yleensä tunnistaa ja sisältö luotettavasti varmistaa. [193]

Tietoverkon välityksellä tehtävien oikeustoimien osalta muotovaatimusten täyttyminen ei kuitenkaan ole itsestäänselvyys. Tekijän tunnistaminen ja sisällön varmentaminen edellyttävät osapuolten välillä etukäteen sovittuja menettelytapoja tai riittävät vaatimukset täyttävän sähköisen allekirjoituksen käyttämistä.

6.1 Pääsääntönä muotovapaus

Oikeustointen tekemisessä on Suomessa voimassa muotovapauden periaate. Sopimus voidaan lähtökohtaisesti tehdä sopijapuolien haluamassa muodossa. Suomalaisessa lainsäädännössä sähköisen sopimuksen käsitettä ei tunneta[194], joten ei ole oikeudellista estettä sille, että sopimus voidaan tehdä pätevästi myös sähköisessä muodossa.[195] Varallisuusoikeudellisista oikeustoimista annetun lain ensimmäinen luku sisältää sopimuksen tekemistä säätelevät lainkohdat ja sellaiset yleisperiaatteet, joita voidaan pitää sopimuksen tekemisen perusperiaatteina myös muilla oikeusjärjestyksen aloilla.[196]

---

[192] Hemmo 2003 s. 181–182.
[193] Laine (toim.) 2001 s. 195–196.
[194] Nurmi 1997 s. 9. Oikeustoimilakitoimikunta (1990:20) käyttää tutkimuksen kohteena olevasta laitteistoa muotoilua "uusi tiedonsiirtotekniikka".
[195] HE 194/2001 s. 12. Varallisuusoikeudellisista oikeustoimista annetussa laissa (228/1929), jäljempänä oikeustoimilaki, on sopimuksen tekemistä koskevat keskeiset säädökset.
[196] Hoppu – Hoppu 2007 s. 31.

OiKTL:n mukaan sopimus syntyy, kun tehtyyn tarjoukseen on saatu sitä vastaava, hyväksyvä vastaus. Tarjous tai vastaus voidaan lähtökohtaisesti antaa missä muodossa tai millä välineellä tahansa, edellyttäen etteivät sopijapuolet ole keskenään sopineet tietyn muodon noudattamisesta.

Suurin osa yksityisoikeudellisista oikeustoimista on sopimusten perusteella muotovapaita. Verkon välityksellä tehty sähköinen sopimus on siis lähtökohtaisesti yhtä pätevä kuin esimerkiksi kirjallinen sopimus. Kirjallinen muoto olisi kuitenkin suositeltava, jotta sitoumuksen antamisen ja sisällön voisi todistaa. Siksi yksityisoikeudellisia sopimuksia verkossa toteutettaessa sopimusvapaus ja vapaa todistusharkinta tarjoavat hyvän mahdollisuuden käyttää sähköisiä allekirjoituksia ja varmenteita.[197] Käytännössä sähköisten sopimusten muodossa annettavat sopimusilmaisut yleensä ovat sopimustyyppiä, joiden osalta ei ole laissa säädetty tiettyä määrättyä muotoa.[198]

6.2 Muotovaatimuksellinen sähköinen sopimus

Muotovapaus ei ole voimassa poikkeuksetta. Suomen lainsäädännössä on runsaasti kirjallista muotoa koskevia vaatimuksia, jotka liittyvät sopimuksen tekemiseen, vakiosopimusehtoihin, osapuolten välisiin ilmoituksiin tai sopimuksen päättämiseen liittyvään menettelyyn. Muotovaatimukset ovat tarpeellisia silloin, kun sopimuksilla aikaan saatavat oikeusvaikutukset halutaan rekisteröidä. Myös sopimusperusteiset muotovaatimukset (muotovaraumat) ja niiden syrjäyttämisen luomat oikeusvaikutukset on otettava huomioon. Sovitun muotovaatimuksen syrjäyttämisen seuraus riippuu siitä, mikä on ollut sille asetettu tarkoitus muotovaatimusta määrättäessä.[199]

Muotovaatimus voi koostua useista eri elementeistä tai niiden yhdistelmistä, kuten esimerkiksi 1) kirjallinen asiakirja, 2) allekirjoitettu asiakirja, 3) allekirjoitettu ja päivätty asiakirja, 4) allekirjoitettu, päivätty ja todistettu asiakirja, 5) osapuolten

---

[197] HE 197/2001 s. 7.
[198] Nurmi 1997 s. 100.
[199] Nurmi 1997 s. 111.

samanaikainen läsnäolo sopimusta päätettäessä, 6) viranomaisen vahvistama asiakirja tai 7) oikeustoimella siirrettyjen oikeuksien rekisteröinti.[200]

Muotovaatimukset pohjautuvat pitkälti kansallisiin lakeihin. Kansainvälisiin sopimusvelvoitteisiin sovelletaan EU-maissa ratifioitua Rooman yleissopimuksen 9 artiklan määräystä, jonka mukaan sopimukseen sovellettava laki tai sopimuksen tekopaikan laki määrää sopimukseen liittyvät muotovaatimukset.[201]

Muotovaatimuksia on lakisääteisiä ja sopimusperusteisia. Sopimusperusteisia muotovaatimuksia kutsutaan muotovaraumaksi. Suomalaisen oikeuskirjallisuuden mukaan muotovaatimukset voidaan jakaa varsinaisiin, epävarsinaisiin ja ohjesisältöisiin muotosäännöksiin. [202] Varsinaisten muotosäännösten noudattaminen on edellytys pätevän sopimuksen syntymiselle.[203] Varsinaisesta muotosäännöksistä voidaan mainita esimerkkinä maakaaren 2 luvun 1 § mainittu kirjallisesti tehtävä kiinteistönkauppa.

Epävarsinaisen muotosäännöksen noudattamatta jättämisestä aiheutuu osapuolelle jokin muu haitallinen oikeusvaikutus kuin sopimuksen aineellisoikeudellinen pätemättömyys.[204] Esimerkkinä voidaan mainita moottoriajoneuvon kauppa. Kauppa on sitova suullisenakin, mutta ostaja ei saa ajoneuvoa rekisteröityä omiin nimiinsä, ellei hän esitä luovutuskirjaa.

Ohjesisältöinen muotosäännös liittyy oikeustoimen syntymisen ja sisällön todentamiseen. Ohjesisältöisen muotosäännöksen syrjäyttänyt osapuoli kärsii haitalliset seuraamukset siitä, ettei tahdonilmaisun antamisesta tai sen sisältöä pystytä myöhemmin todistamaan. Ohjesisältöiset muotosäännökset ovat vain neuvoa antavia, joten niiden avulla voidaan pyrkiä tarkentamaan kuinka osapuolten olisi tarkoituksenmukaista menetellä sopimusta solmittaessa.[205] Ohjesisältöisestä

---

[200] Laine (toim.) 2001 s. 198–199.
[201] Railas 2005 s. 1277.
[202] Railas 2005 s. 1276. Suomalaisessa kirjallisuudessa esitetty jako pätee varsin usein myös kansainvälisessä tarkastelussa.
[203] Hemmo 2003 s. 185.
[204] Hemmo 2003 s. 197.
[205] Hemmo 2003 s. 197 ja Railas 2005 s. 1276.

lakisääteisestä muotosäännöksestä käy esimerkkinä huoneenvuokralakien yleisluonteinen määräys, jonka mukaan vuokrasopimus ja sen muutos on tehtävä kirjallisesti. Muotosäännöksen syrjäyttämisellä ei ole vaikutusta toistaiseksi voimassa olevan vuokrasuhteen pätevyyteen.[206]

6.2.1 Muotovaatimuksena kirjallinen sopimus tai allekirjoittaminen

Yksityisoikeudellisten sopimusten osalta on kirjallinen muoto ja allekirjoitusvaatimus yleisimmin käytettyjä muotovaatimuksia. Ilmaisuja "kirjallisesti" tai "allekirjoittaa" ei ole määritelty tarkemmin lainsäädännössä.[207] Perinteinen asiakirjan allekirjoitus menettää sähköisen tiedonsiirron yhteydessä ilmaisun alkuperäisyyttä osoittavan ominaisuuden. Sähköisessä muodossa siirrettyjä asiakirjoja voidaan myös kopioida asiakirjan alkuperäisyyden hämärtävin seurauksin.[208]

Kehittyneimpiin todentamis- ja suojausmenetelmiin perustuvat sähköiset allekirjoitukset täyttävät allekirjoituksen identifiointi- ja autenttisuustehtävänsä jopa selvästi perinteistä omakätistä allekirjoitusta tehokkaammin.[209] Perinteisen omakätisen allekirjoituksen kopioiminen on nykyään tekniikan kehityttyä helpottunut huomattavasti. Vähintään perinteisen omakätisen allekirjoituksen varmuustason turvaavat sähköiset allekirjoitukset on siis hyväksyttävä tehokkaiksi allekirjoituksiksi. Esimerkiksi asymmetriseen kryptaukseen perustuva sähköinen allekirjoitus täyttää kiistatta allekirjoituksen funktiot perinteistä paperille tehtävää allekirjoitusta paremmin.[210]

Tietoyhteiskunnan palvelujen tarjoamisesta säädetyn lain 12.1 §:ssä säädetään, että vaatimus sopimuksen tekemisestä kirjallisesti voidaan täyttää sellaisella sähköisellä sopimuksella, jonka sisältöä ei voida yksipuolisesti muuttaa ja joka säilyy osapuolten

---

[206] Laine (toim.) 2001 s. 199.
[207] HE 197/2001 s. 7 ja 12.
[208] Nurmi 1997 s. 99–100.
[209] Sähköisille allekirjoituksille asetettavista vaatimuksista ja niiden teknisestä toteuttamisesta katso Laine (toim.) 2001 s. 205–212.
[210] Nurmi 1997 s. 101–103.

saatavilla. Vaatimuksen täyttää esimerkiksi sähköpostitse tehty sopimus, joka on allekirjoitettu sähköisesti siten, että sisällön muuttumattomuus on varmistettavissa.[211]

Laissa sähköisistä allekirjoituksista (24.1.2003/14) 18§:n yleissäännöksellä varmistetaan, että ainakin laatuvarmenteeseen perustuva ja turvallisen allekirjoituksen luomisvälineen avulla luotu sähköinen allekirjoitus samaistetaan perinteiseen, käsintehtyyn allekirjoitukseen. Millainen tahansa sähköinen allekirjoitus voidaan luonnollisesti myös riitauttaa vastaavasti kuin perinteinen käsintehtykin allekirjoitus.[212]

6.2.2 Sopimussuhteessa todisteellisesti toimitettavat ilmoitukset

Suomen lainsäädännössä on määritelty tietoyhteiskunnan palvelujen tarjoamisesta (5.6.2002/458) säädetyllä lailla, että sopimussuhteeseen liittyviä ilmoituksia, jotka on lain mukaan toimitettava todisteellisesti, voidaan myös toimittaa sähköisesti tiettyjen edellytysten täyttyessä. Tällaisia oikeustoimia ovat esimerkiksi ilmoitukset asuinhuoneiston ja liikehuoneiston vuokrasopimuksen irtisanomisesta. Käytetyn menetelmän on mahdollistettava ilmoituksen vastaanottamisen todentaminen. Sähköisen vastaanottokuittauksen käyttämisen täyttää kuittaus, jonka vastaanottaja on allekirjoittanut kehittyneellä sähköisellä allekirjoituksella, joka perustuu laatuvarmenteeseen ja on luotu turvallisella allekirjoituksen luomisvälineellä.

Mahdollisuus täyttää laissa säädetyt kirjallisen muodon vaatimukset ja allekirjoitusvaatimukset sähköisesti koskee myös sopimussuhteen aikana toimitettavia osapuolten ilmoituksia sekä muita sopimukseen liittyviä toimenpiteitä.[213] Tällainen ilmoitus voidaan toimittaa myös sähköisesti, edellyttäen että ilmoituksen vastaanottaminen on jälkikäteen näytettävissä toteen.

---

[211] HE 194/2001 s. 37.
[212] HE 197/2001 s. 35.
[213] HE (194/2001) 37/57 12.2 §.

6.3 Poikkeukset ja rajoitteet

Sähköisen kaupankäynnin direktiivissä (2000/31/EY) on annettu jäsenvaltioille mahdollisuus säätää poikkeuksia pääsääntöön seuraavien sopimustyyppien osalta:

- sopimukset, joilla luodaan tai siirretään oikeuksia kiinteään omaisuuteen vuokraoikeuksia lukuun ottamatta
- sopimukset, jotka lain mukaan edellyttävät tuomioistuimen, viranomaisten tai julkista valtaa käyttävien ammatinharjoittajien myötävaikutusta
- luonnollisten henkilöiden muutoin kuin ammattitoiminnassa myöntämät henkilö- tai esinevakuussopimukset
- perhe- ja jäämistöoikeudelliset sopimukset

Sähköisen kaupankäynnin direktiivin (2000/31/EY) mukaan jäsenvaltioiden on kuitenkin pidettävä huoli siitä, että niiden oikeusjärjestelmässä annetaan mahdollisuus sopimusten tekemiseen sähköisessä muodossa. Jäsenvaltioiden on erityisesti varmistettava, ettei sopimuksentekomenettelyyn sovellettavilla oikeudellisilla vaatimuksilla aseteta esteitä sähköisessä muodossa tehtävien sopimusten käytölle.

Direktiivin mukaan lainsäädännön muuttamista koskevan tarkastelun tulee tapahtua systemaattisesti siten, että sen on koskettava kaikkia sopimuksentekomenettelyn vaiheita, mukaan lukien sopimuksen rekisteröinti. Jäsenvaltioiden velvollisuus poistaa esteet sähköisesti tehtyjen sopimusten käytöltä koskee siis vain esteitä, jotka johtuvat oikeudellisista vaatimuksista, ei esteitä jotka johtuvat siitä että sähköistä muotoa on tietyissä tapauksissa mahdotonta käyttää.[214]

Direktiivillä ei kuitenkaan rajoiteta jäsenvaltioiden mahdollisuutta asettaa tai pitää voimassa sopimuksia koskevia yleisiä tai erityisiä vaatimuksia, jotka voidaan täyttää sähköisessä muodossa. Tietyissä erityistilanteissa muotomääräyksen noudattaminen on

---

[214] 2000/31/EY.

asetettu sopimuksen pätevyyden edellytykseksi, jolloin osapuolet eivät voi solmia pätevää sopimusta muotomääräystä noudattamatta.[215]

Suomen lainsäädännössä on määritelty tietoyhteiskunnan palvelujen tarjoamisesta (5.6.2002/458) säädetyllä lailla, että kyseistä lakia ei sovelleta kiinteistön kauppaan tai muuhun luovutusta koskevaan sopimukseen.[216] Sähköisessä muodossa ei ole mahdollista solmia perhe- tai jäämistöoikeudellisia sopimuksia, kuten avioehto-, ositus- tai perinnönjakosopimuksia.[217]

6.4 Sähköisen sopimuksenteon muotovaatimuksiin liittyvät edut ja haitat

Sähköisiin sopimuksiin liittyvät käsitteet ja tietotekniikkaan liittyvät erityispiirteet ovat avanneet uusia näkökulmia perinteisen sopimusjuridiikan näkökulmasta katsottuna. Suurin osa sähköisistä sopimuksista ja kaupankäynnistä tapahtuu avoimissa tietoverkoissa. Osapuolet eivät ole etukäteen sopineet tunnistamiseen ja sisällön varmentamiseen liittyviä menettelytapoja. Tämä luo paineita muotovaatimusten täyttämiselle, joten kyseisissä tilanteissa sähköisellä allekirjoituksella ja sopimuksen sisällön todentamisella on suuri rooli.

Erityispiirteisiin on luettava tietyissä tilanteissa mahdolliset epävarmuustekijät. Esimerkiksi sopimusilmaisu, joka antaa antajansa tahtoa vastaamattoman sisällön esimerkiksi antajan oman, tietokoneen virheen tai tiedonsiirron aikana syntyneen virheen takia.[218] Epävarmuuksista johtuen riskinjako on tahdon ohella merkittävä sähköisen sopimusilmaisun sitovuuteen vaikuttava tekijä. Virhetilanteissa joudutaan lähtökohtaisesti käyttämään "olisi pitänyt havaita" –tyyppisiä, tulkinnanvaraisia ratkaisuperusteita.[219]

---

[215] Laine (toim.) 2001 s. 201.
[216] Kiinteistön luovutus voidaan tehdä vain maakaaren (540/1995) 2§ luvun 1:n säädetyllä tavalla.
[217] Mm. 1074/2000 5§, 119/2001 21§, 313/2001 24§ ja 55/2001.
[218] Nurmi 1997 s. 106.
[219] Nurmi 1997 s. 106–111.

Sosiaalisen elementin puuttumisen vuoksi ihmiset eivät välttämättä koe digitaalista allekirjoitusta yhtä velvoittavaksi kuin omakätisen allekirjoituksen. Omakätisen allekirjoituksen tekemiselle on ominaista allekirjoituksen seremoniaalinen ominaisuus, kun taas sähköinen allekirjoitus tehdään käytännössä painamalla esimerkiksi selaimen tilaa tai sähköpostin allekirjoita -painiketta.[220] Sähköisen allekirjoituksen luomiseen liittyy myös useampia vaiheita kuin allekirjoituksen luomiseen käsin.

Muotosäännösten haittana on pidetty sitä, että ne ovat epämukavia noudattaa ja hidastavat oikeustoimen tekemistä. Muotovaatimuksen noudattamiseen liittyy myös erehtymisen mahdollisuus. Muotovirheen seurauksena oikeustoimella tavoitellut vaikutukset voivat jäädä saavuttamatta. Muotovaatimuksista aiheutuu myös usein suullista sopimusta suuremmat kustannukset.[221]

Sähköisen sopimuksenteon muotovaatimuksilla edistetään myös oikeusvarmuutta. Oikeusvarmuuteen liittyen muodon etuina on mainittu todistettavuuden edistäminen, tahdonilmaisun oikeaperäisyyden varmistaminen ja materiaalisten vääryyksien estäminen. Osan todentamisvaatimuksista sähköinen allekirjoitus täyttää jopa omakätistä allekirjoitusta paremmin. Muotosäännöksen on myös katsottu kiinnittävän tahdonilmaisun antajan huomion oikeustoimen taloudelliseen merkitykseen ja toimeen liittyviin riskeihin.[222]

Muotovaatimusten merkitystä sopimuksessa arvioitaessa on huomioitava, että varsinaisen muotovaatimuksen noudattaminen on edellytys pätevän sopimuksen syntymiselle. Epävarsinaisen muotovaatimuksen noudattamatta jättäminen aiheuttaa osapuolelle jonkun muun haitallisen oikeusvaikutuksen kuin sopimuksen pätemättömyyden. Ohjesisältöinen muotovaatimus liittyy oikeustoimen syntymiseen ja sisällön todentamiseen. Osapuoli, joka syrjäyttää ohjesisältöisen muotovaatimuksen kärsii haitalliset seuraamukset siitä, ettei tahdonilmaisua tai sen sisältöä pystytä myöhemmin todentamaan.[223]

---

[220] Laine (toim.) 2001 s. 213–214.
[221] Hoppu – Hoppu 2007 s. 58 ja Kivimäki – Ylöstalo 1981 s. 301.
[222] Nurmi 1997 s. 106–107.
[223] Laine (toim.) 2001 s. 199.

Oikeuksia luovien tahdonilmaisujen osalta sähköisen ilmaisun kantajalla on riski omasta ja tietokoneen hänen puolestaan tekemästä virheestä ja myös elektronisen tiedonsiirron häiriön seurauksena syntyneestä virheestä. OikTL:n 32.1:n mukaan vääristynyt tahdonilmaisu sitoo ilmaisun antajaa sen sisällön mukaisena, mikä ilmaisulla oli sen kohteelle saapuessa, edellyttäen ettei ilmaisun vastaanottaja tiennyt eikä hänen olisi pitänyt tietää virheestä. Sopijapuolet voivat tahtoessaan muuttaa virhetilanteiden riskinjakoa kytkemällä riskinjaon sovitun teknisen muotovaatimuksen noudattamiseen.[224]

Teknisen muotovaatimuksen huomioimatta jättämisestä voi seurata tapauskohtainen intressivertailuun perustuva sanktio. Vastapuolen sovitun muodon vastaisesta toiminnasta aiheutuvista epäsuotuisista vaikutuksista ei saa kärsiä se sopijapuoli, jonka intressiä muotovaatimuksen noudattaminen suojaa. Pätemättömyys, vahingonkorvaus tai sopimussakko voi olla seurauksena muotovaatimuksen huomioimatta jättämisestä, riippuen tapauksesta ja sopimusilmaisusta.[225]

---

[224] Nurmi 1997 s. 114.
[225] Nurmi 1997 s. 115.

7. Sähköisiin sopimuksiin liittyviä erityiskysymyksiä

7.1 Tekniset ongelmat

Sähköisten sopimusten yhtenä ongelmana voidaan pitää teknologiaan liittyviä ongelmia; katkenneet yhteydet tai muut tiedonsiirtovirheet voivat johtaa suureen määrään keskeneräisiä tahdonilmaisuja, joiden oikeusvaikutuksista voi olla vaikea sanoa mitään varmaa. On mahdollista että verkossa lähetetty tahdonilmaisu jää kokonaan tulematta vastaanottajalle tai että se saapuu perille vain osittain. Verkon ylikuormittuessa tai muun odottamattoman viivästyksen takia ilmaisu voi jäädä saapumatta perille määräaikaan mennessä. Mikä on oikea toimintatapa ja kuka kantaa vastuun?

Perinteisen sopimusteorian mukaan katsotaan ilmaisun olevan lähettäjän valtapiirissä, kunnes se on saapunut joko vastaanottajan tai hänen lähipiirinsä saataville. Tähän asti lähettäjä vastaa tiedon saapumisesta adressaatille. Tämän mukaisesti voidaan katsoa, että mikäli vastaus saapuu myöhässä, tämä on lähettäjän vastuulla eikä sopimusta siis ole syntynyt.[226]

On mahdollista että lähettäjä ei havaitse mitään ongelmaa ja uskoo tahdonilmaisunsa saavuttaneen vastaanottajan. Varallisuusoikeudellisista oikeustoimista annetun lain 4 §:ssä todetaan, että sopimus voi myös syntyä myöhästyneen vastauksen oikeusvaikutuksesta siinä tapauksessa, että vastauksen lähettäjä on olettanut vastauksen tulleen oikeassa ajassa perille ja vastauksen saajan on täytynyt tämä käsittää.[227] Kyseisessä tapauksessa vastauksen saajan on viipymättä ilmoitettava vastauksen myöhästymisestä ja siitä että hän ei halua hyväksyä sopimusta. Muuten sopimus katsotaan syntyneeksi. On kuitenkin epäselvää, milloin vastaanottajan olisi täytynyt käsittää lähettäjän luottaneen siihen, että ilmaisu saapuu perille ajoissa. Esimerkiksi sähköpostista on mahdollista tarkastaa lähetysaika heti sen saavuttua ja katsoa, viittaisiko se siihen mahdollisuuteen, että vastauksen on uskottu ehtivän ajoissa. Mitään yleistä sääntöä ei kuitenkaan ole, vaan kyse on hyvin pitkälti tapauskohtaisuudesta.

---

[226] Nurmi 1997 s. 40.
[227] Laki varallisuusoikeudellisista oikeustoimista (228/1929) 4 §.

Sähköisessä sopimisessa on myös mahdollista, että tahdonilmaisu ei saavu ehjänä kokonaisuutena, vaan osa siitä katoaa matkalla. On tulkittu, että tällaisessa tilanteessa kyseessä ei yleensä ole itsenäinen tahdonilmaisu ennen kuin se on vastaanotettu kokonaan, jolloin oikeusvaikutusta ei synny ennen kuin loputkin ilmaisusta on saapunut vastaanottajalle. Poikkeuksena voi kuitenkin olla tilanne, missä vastaanotetusta osasta käy ilmi esimerkiksi tarjouksen hyväksyminen. Tällöin se voidaan tulkita itsenäiseksi ilmaisuksi ja näin ollen hyväksyä sellaisenaan, jolloin sopimus syntyy jo kyseisen osan vastaanottohetkellä.[228]

Mikäli tahdonilmaisun vastaanotossa tapahtuu ongelmia, oikeusvaikutus syntyy yleensä tästä huolimatta. Lähettäjän pitää kuitenkin pystyä todistamaan adressaatin estäneen tahdonilmaisun perille tulon. Tällainen tilanne voi syntyä esimerkiksi silloin, kun henkilö yrittää lähettää tarjoukseen myöntävää vastausta sähköpostitse, mutta vastaanottajan sähköpostilaatikko on täynnä eikä hän voi vastaanottaa viestiä. Vastaanottaja voisi korjata tilanteen tyhjentämällä postilaatikkonsa, mutta vaikka hän ei tätä tekisikään, sopimusvaikutus katsottaisiin syntyneeksi. Sama pätee myös tarjouksentekijän antamiin viallisiin yhteystietoihin; mikäli ilmaisu ei saavu perille esimerkiksi väärän sähköpostiosoitteen takia, vastaanottajaa voidaan pitää tästä vastuussa.

7.2 Sähköisten sopimusten kansainvälisyys ja lainsäädäntö

Yhtenä Internetin erityispiirteenä voidaan pitää kansallisten fyysisten ja kulttuurirajojen katoamista.[229] Tietyssä maassa ladatut sivut ovat nähtävissä maailmanlaajuisesti, jonka johdosta kuluttajan voi olla vaikea hahmottaa missä maassa elinkeinonharjoittaja sijaitsee. Toisaalta myös elinkeinonharjoittajan on lähes mahdotonta tietää varmasti missä maassa sivustoilla asioivat kuluttajat ovat. Avainkysymykseksi onkin

---

[228] Nurmi 1997 s. 43.

[229] www.tieke.fi / Julkaisut / Oppaat yrityksille / Sähköisen kaupankäynnin aapinen / sähköisen kaupankäynnin oikeudelliset kysymykset / Yritysten välisen sähköisen kaupan oikeudellisia kysymyksiä, 11.2.2008.

muodostunut miten fyysisen maailman oikeudelliset rakenteet, normit ja riidanratkaisumekanismit tulisi sovittaa sähköiseen kaupankäyntiin.[230]

Yritysten välisessä kaupassa sopijapuolet ovat voineet verrattain vapaasti päättää keskinäisistä sopimuksistaan, koska valtioiden intressissä ei ole ollut rajoittaa sopijapuolten sopimusvapautta pakottavalla tai toista osapuolta suojaavalla lainsäädännöllä. Sitä vastoin kuluttajien suojaaminen myös kansainvälisessä kaupassa on herättänyt valtioiden kiinnostuksen.

Valtioiden lainsäädäntövallan rajat ovat häilyvät, eikä kansainvälisestä yksityisoikeudesta ole löytynyt tyhjentäviä vastauksia oikeussuhteissa sovellettaviin lainvalintoihin. Valtioiden välisiä yhteisiä pelisääntöjä, joilla päällekkäisten ja ristiriitaisten lainkäyttöperusteiden aiheuttamia oikeudellisia ristiriitoja voitaisiin korjata, ei ole saatu aikaan.

EU:n jäsenvaltioiden solmimaa Rooman yleissopimusta (SopS 30/1999) ja sen kuluttajansuojanormistoa on sovellettu EU:n tuomioistuimissa lainvalintaa pohdittaessa. Se on suljettu laki, johon voivat liittyä ainoastaan Euroopan yhteisöjen jäsenvaltiot. Soveltamisala on kuitenkin sikäli yleinen, että sen mukaisesti määräytyvää lakia sovelletaan, vaikka kyseessä olisi muun kuin yleissopimusvaltion laki.[231] Rooman yleissopimusta sovelletaan aina kun sopimusvelvoitteilla on liittymä useampaan kuin yhteen valtioon. Tämä liittymä voi johtua niin osapuolen asuinpaikasta, suorituspaikasta kuin keskushallinnon sijaintipaikastakin.

Kansainvälisessä sähköisessä kaupassa elinkeinonrahoittajat liittävät yleensä vakioehtoihinsa lainvalintaa koskevan ehdon, jota kutsutaan lakiviittaukseksi. Yleensä elinkeinonharjoittaja valitsee sovellettavaksi sen EU-maan lainsäädännön, missä se on rekisteröity kaupparekisteriin. Suomessa elinkeinonharjoittaja voi Sähköisen kaupan direktiivin mukaan valita myös sovellettavaksi jonkin toisen jäsenvaltion lainsäädännön. Kuluttajasopimusten kohdalla lakiviittaus Euroopan talousalueen ulkopuoliseen

---

[230] Puurunen 2005 s. 14.
[231] Laine (toim.) 2001 s. 242.

valtioon ei saa johtaa siihen että kuluttaja menettäisi oman asuinvaltionsa pakottavan kuluttajansuojalain myöntämän suojan (KSL 5.29a §). Mikäli mitään lakiviittausta ei ole tehty, sovelletaan kuluttajan kotipaikan lakia ja muita sopimusoikeudellisia normeja.[232]

Tuomioistuinten toimivaltaa tarkastelemalla voidaan yrittää hahmottaa sääntöjä kansainväliseen sähköiseen kauppaan. Esimerkiksi EU-jäsenvaltioiden solmiman Brysselin sopimuksen mukaan kuluttaja voi nostaa kanteen kotipaikkansa tuomioistuimessa, jos sopimuksentekoa on edeltänyt tarjous tai mainontaa kuluttajan asuinpaikkavaltiossa ja kuluttaja on toteuttanut kyseisessä valtiossa sopimuksentekoa varten tarvittavat toimenpiteet. On kuitenkin kovin tulkinnanvaraista onko elinkeinonharjoittaja kohdentanut mainontaa juuri kyseiseen maahan. Euroopan osalta normisto täyttää paremmin oikeusvarmuuden vaatimukset kuin kansainvälisen oikeuden lainsäädäntövallan rajoja sääntelevät normit. Sekä eurooppalaiset että amerikkalaiset tuomioistuimet tarvitsevat tarkempia ja selkeämpiä normeja, joita soveltaa kansainväliseen sähköiseen kauppaan.[233]

Yhdeksi ratkaisuksi onkin ehdotettu yhteisen järjestelmän luomista, jossa elinkeinonharjoittajalla olisi mahdollisuus suunnata toimintansa tiettyihin maihin ja sitoutua noudattamaan kyseisten maiden pakottavaa kuluttajaa suojaavaa lainsäädäntöä. Tilanteessa, jossa elinkeinonharjoittaja solmisi sopimuksen sellaisen valtion kuluttajan kanssa, johon hän ei ole suunnannut toimintaansa, olisi elinkeinonharjoittajalla oikeus viedä riita oman kotivaltionsa tuomioistuimeen ja soveltaa sopimuksessa määrättyä lakia. [234]

Kynnys viedä riita tuomioistuimeen kansainvälisessä sähköisessä kaupassa on korkea, riidan ratkaisun kustannuksien ylittäessä yleensä riidan arvon. Riidanratkaisu on liian hidasta ja kallista. Yhdysvalloissa ja Euroopassa on kehitelty kansainvälisiä ja yksityisiä Internetissä toimivia riidanratkaisupalveluja. Ne tarjoavat edullisemman tavan ratkaista kuluttajien ja elinkeinonharjoittajien välisiä riitoja. Palveluista aiheutuvat kustannukset,

---

[232] Laine (toim.) 2001 s. 243.
[233] Puurunen 2005 s. 14.
[234] Puurunen 2005 s. 14.

palveluiden läpinäkyvyys ja valvonnan puute eivät yleensä täytä oikeusvaltion riidanratkaisulle edellyttämiä vähimmäisvaatimuksia.

7.3 Vakioehdot sähköisessä sopimuksessa

Vakioehdot ovat ehtoja, jotka laaditaan käytettäväksi useissa yksittäisissä tulevaisuudessa solmittavissa sopimuksissa ja joita on tarkoitus käyttää erilaisten sopimuskumppaneiden kanssa. Vakioehtojen sopimuksen osaksi tulemiselle on kaksi ehtoa. Ensimmäiseksi vakioehtoihin pitää nimenomaisesti viitata sopimusta päätettäessä. Toiseksi osapuolella, joka ei ole ehtoja laatinut, pitää olla mahdollisuus tutustua ehtoihin ennen sopimuksen lopullista solmimista. Vakioehtoja tarkastellessa tulee erottaa yksipuolisesti laaditut vakioehdot ja sopijapuolien tai näiden edustajien yhteisesti laatimat vakioehdot toisistaan.[235]

7.3.1 Yksipuolisesti laaditut vakioehdot

Yksipuolisesti laadittuja vakioehtoja noudatetaan lähes poikkeuksetta kuluttajan ja palveluntarjoajan välisissä massaluonteisissa sähköisissä sopimuksissa. Osapuolten välillä on harvemmin suoraa aitoa kahdenkeskistä vuorovaikutusta sopimusten massavaihdannasta johtuen. Kuluttajalla myöskään harvemmin on mahdollisuutta vaikuttaa sopimusehtojen sisältöön joukkomittaisissa sähköisissä sopimuksissa, koska ne ovat yksipuolisesti toisen osapuolen laatimia. Kuluttajan mahdollisuudet rajoittuvat lähinnä ehtojen hyväksymiseen, joka johtaa kaupan hyväksymiseen tai ehtojen hylkäämiseen aiheuttaen sopimuksenteon keskeytymisen.[236]

Elinkeinoharjoittajan on tuotava vakioehdot asiakkaan nähtäville ja hyväksyttäväksi helppokäyttöisellä tavalla.[237] Vakioehtoihin viittaaminen on toteutettava siten, että asiakas voi vaivattomasti havaita elinkeinonharjoittajan tarkoittavan sopimuksen

---

[235] Hemmo 2003 s. 146–151.
[236] Nurmi 1997 s. 119.
[237] Direktiivi 97/7/EY kuluttajansuoja etäsopimuksissa 4 artiklan 2 kohta: "Artiklan 1 kohdassa tarkoitetut tiedot, joiden kaupallisesta tarkoituksesta ei saa olla epäselvyyttä, on annettava selkeinä ja ymmärrettävinä käytettyyn etäviestintävälineeseen soveltuvalla tavalla".

tekemistä vakioehdoin. Sopimuksen ehdot on tarjottava asiakkaalle sellaisessa muodossa, että ne on mahdollista tallentaa, tulostaa ja myöhemmin toisintaa samanlaisina (TietoyhtPalvL 9 §).

Vakioehdot voivat olla asiakkaan nähtävillä esimerkiksi tietyn kuvakkeen takana, tulla automaattisesti ruudulle ennen sopimuksentekoprosessin jatkamista tai asiakkaan on selattava ehdot läpi ja hyväksyttävä ne ennen kuin hän voi jatkaa sopimuksentekoprosessia. Sopimuksentekotekniikan yksityiskohdilla ei yleensä liene ratkaisevaa merkitystä vakioehtojen pätevyyteen, vaan olennaista on että asiakkaalle on tarjottu helppokäyttöinen mahdollisuus tutustua ehtoihin.[238] Esimerkiksi hyperlinkkien takana olevan tiedon ei ole katsottu täyttävän helpon saatavuuden vaatimusta, vaan sopimusehtojen tulee olla kiinteästi yhteydessä sivustoon, jossa sopimus tehdään. Hyväksyttämällä vakioehdot asiakkaalla elinkeinonharjoittaja varmistaa asiakkaan olevan tietoinen sopimukseen liitetyistä vakioehdoista.

Kuluttajalle pyritään takaamaan suomalaisessa oikeusjärjestyksessä tietty vähimmäissuoja, esimerkiksi epäselvien tai hyvin tulkinnanvaraisten vakioehtojen osalta siten että ehtoja tulkitaan laatijan eli elinkeinoharjoittajan tappioksi.[239] Epätavallisista tai ankarista sopimusehdoista on myös huomautettava erikseen. Kuluttajasopimusten osalta elinkeinonharjoittajalle on asetettu näyttövelvollisuus siitä, että kysymyksessä on yksilöllisesti laadittu sopimus.[240]

7.3.2 Sopijapuolien tai näiden edustajien yhteisesti laatimat ehdot

Vakioehtojen syntyessä molempien sopijapuolien yhteisen intressin pohjalta on vakioehtojen liittäminen sopimuksen osaksi luontevaa. Vakioehtojen käytön avulla saadaan dispositiiviseen lainsäädäntöön verrattava vaikutus ja sopimussuhteen ennalta arvattavuus kasvaa. Käytettäessä vakioehtoja sopimusta solmittaessa on usein ongelma, että osapuolet eivät ole täysin tasavertaisessa asemassa, ehtojen yhteinen valmistelu on

---

[238] Hemmo 2003 s. 150.
[239] Nurmi 1997 s. 119.
[240] KSL:n 4:4 (Säädös perustuu direktiiviin kuluttajasopimusten kohtuuttomista ehdoista, artikla 3.2.3).

voinut olla näennäistä ja todellinen vaikutusvalta yksipuolista.[241] Vakioehtojen laatijalla on selkeä etulyöntiasema, sillä hän on voinut muotoilla ehdot itsensä kannalta hyvinkin edullisiksi eikä toisella osapuolella useinkaan ole mahdollisuutta vaikuttaa niiden sisältöön.

Ongelmaksi voi muodostua yksilöllisten ehtojen ja vakioehtojen erottamiseen liittyvät näyttökysymykset. Toinen sopijapuoli voi väittää, että tietokoneen muistista tulostetut ehdot on laadittu yksilöllisesti ja yhteisesti sopijapuolien kesken erityisesti kyseistä sopimussuhdetta varten.[242]

7.4 Tietoturvallisuus ja yksityisyydensuoja sähköisessä kaupankäynnissä

Internetin normaalissa tiedonsiirrossa käytettäviin tiedonsiirtoprotokolliin ei ole rakennettu valmiiksi tietoturvamekanismeja eli tieto liikkuu suojaamattomassa muodossa, vertausta postikortin tietoturvaan voidaan pitää osuvana.[243] Tietoliikenteen suojaamiseen löytyy monia keinoja, esimerkiksi Secure Sockets Layer (SSL) salausprotokolla[244] ja IPSec (Internet Protocol Security Architecture) protokolla, jotka ovat vakiinnuttaneet asemansa tavallisimpana tapana suojata tietoliikennettä.[245] Tietoliikenteen suojaaminen toteutetaan kuitenkin palvelukohtaisesti ja suojauksen taso vaihtelee huomattavasti. Nimipalvelimiin ja reitittimiin on mahdollista murtautua, datapaketteja on mahdollista kerätä talteen tai reitittää uudelleen. Murto-ohjelmien yleistyessä kuvatunlaiset ongelmat ovat mahdollisia ja riski joutua rikoksen uhriksi on kasvanut. Internetissä epävarmuutta viestin lähettäjästä, identiteetistä, sanoman muuntumattomuudesta ja sen tarkoituksesta voidaan pitää suurempana kuin mitä normaalisti kohtaamme.[246] Kuluttajan suurimmaksi ongelmaksi sähköisessä kaupankäynnissä Internetissä on muodostunut elinkeinonharjoittajan yksilöinti luotettavasti.

---

[241] Hemmo 2003 s. 147.
[242] Nurmi 1997 s. 121
[243] Terämaa (toim. Laine) 2001 s. 42
[244] SSL-salausprotokollaa tukevat yleisimmät Internet-selaimet ja WWW-palvelinohjelmistot.
[245] Rinne 2002 s. 145. Sekä SSL- että IPSec protokolla sisältävät julkisen avaimen salausmenetelmään perustuvan tunnistemekanismin.
[246] Terämaa (toim. Laine) 2001 s. 42

Tietoverkoissa tietojamme kerätään jo nyt lukuisiin eri rekistereihin ja tietokantoihin, joissa olevia tietoja voidaan käyttää ilman suostumustamme tarkoituksiin, joita emme vielä arvaakaan. Verkkopalvelut tekevät tietojen keräämisen entistä helpommaksi. Millä tavalla 10 tai 25 vuoden päästä suhtaudutaan nykypäivänä kerättyihin tietoihin? Ovatko poliittiset ja yhteiskunnalliset olot muuttuneet? Lisääntyvään valvontaan ja rekistereihin tulisi suhtautua kriittisesti ja on kysyttävä aina onko saatavat hyödyt suurempia kuin itse uhkakuvat.[247]

[247] Järvinen 2003 s. 219.

8. Yhteenveto ja johtopäätökset

Sähköisten sopimusten ja kaupankäynnin murros alkoi jo vuosituhannen vaihteessa mutta sähköinen toimintaympäristö tarjoaa edelleen mahdollisuuksia kasvuun ja uusien liiketoimintamallien toteuttamiseen. Sähköisen kaupan kasvun perusedellytyksinä voidaan pitää luottamuksen ja oikeusvarmuuden lisäämistä, joten sähköisiä sopimuksia tulisi olla mahdollista tehdä eri osapuolten välillä yksinkertaisin ja luotettavin sopimusmenettelyin. Uudenlainen toimintaympäristö, jossa fyysisiä tai kulttuurillisia rajoitteita ei perinteisessä mielessä ole, on luonut lainsäätäjille joukon uusia oikeudellisia ongelmia.

Maailmanlaajuisella tasolla voidaan sähköisten sopimusten oikeudellisen sääntelyn ja luottamuskysymysten osoittaa olevan edelleen sekavassa tilassa. Maailmanlaajuinen mallilainsäädäntö ja eri sopimusjärjestelmät eivät ole kovinkaan yhteneväisiä, joten sähköisten sopimusten hyödyntäminen täydessä laajuudessa on vaikeata. Sähköisen kaupankäynnin toimintaympäristössä esiintyy edelleen Villin lännen -ilmapiiristä saatuja vaikutteita, jotka ilmenevät tilanteina, joissa lainsäädäntöä ei ole tai sitä ei haluta noudattaa. Sähköisten sopimusten käytön lisääntyminen on edesauttanut jonkin asteista kehitystä ja karsimista ristiriitaisten kansallisten lainsäädösten osalta. Kehitys tapahtuu yrityksen ja erehdyksen kautta, minkä johdosta heikoimmat järjestelmät katoavat vähitellen paremmin toimivien tieltä.

Kansallisella ja yhteisötasolla toimittaessa sähköisten sopimusten oikeusvarmuus suomalaisen kuluttajan tai elinkeinonharjoittajan näkökulmasta alkaa olla varsin hyvä, johtuen EU:n sähköisiä sopimuksia koskevasta kattavasta lainsäädännöstä ja kuluttajalle korkean suojan tarjoavasta Suomen kuluttajansuojalaista.

Kuluttajille sähköiset sopimukset tarjoavat nykyään nopean tavan asioiden hoitamiseen. Monet arkipäiväiset oikeustoimet, kuten vaikka esimerkiksi lainan hakeminen, vakuutuksen ottaminen ja tuotteiden ostaminen verkosta on mahdollista toteuttaa sähköisessä muodossa. Kuluttaja ei ole sidottu kotimaan markkinoihin, vaan käytössä on globaalit markkinat. Pakottavaa lainsäädäntöä oleva kuluttajansuojalaki asettaa

Suomessa sähköisen sopimuksen tekevän kuluttajan täysin samaan asemaan kuin muita sopimuksentekotapoja käyttävän.

Kun kuluttaja tekee sähköisen sopimuksen EU:n alueelta olevan elinkeinonharjoittajan kanssa, sovelletaan myös kuluttajan kotimaan lainsäädäntöä. Kuluttajan on kuitenkin hyvä muistaa, että ongelmatilanteissa reklamointi käytettävästä kielestä ja kulttuurista johtuen, voi olla kuitenkin huomattavasti hankalampaa ja työläämpää.

Globaalissa kuluttajankaupassa ongelmaksi on muodostunut epätietoisuus ja tulkinnanvaraisuus sovellettavasta lainsäädännöstä, elinkeinoharjoittajan sijaintipaikasta sekä riitatilanteessa toimivaltaisen tuomioistuimen löytämisestä. On muistettava, että kynnys riitauttamiseen kansainvälisessä kuluttajankaupassa on aina korkea riitauttamisen korkeiden kustannusten vuoksi. Voidaankin sanoa, että kuluttajan tulee ymmärtää vastuunsa tekemistään sopimuksista, koska ulkomaisen elinkeinonharjoittajan ollessa petollinen tai kyseisen tahon syyllistyessä sopimusrikkomukseen, ei viranomaisista välttämättä ole apua.

Elinkeinonharjoittajille, erityisesti pienille, kynnys maailmanlaajuisille markkinoille lähtemiseen on huomattavasti matalampi, jos aluevaltaus tehdään sähköisesti. Yritysten välisessä kansainvälisessä kaupassa sopijapuolet voivat verrattain vapaasti päättää keskinäisistä sopimuksistaan ja siitä, minkä maan lainsäädäntöä sovelletaan ja mitä tuomioistuimia käytetään riitatilanteessa.

Vaikkakin sähköisiä sopimuksia koskeva lainsäädäntö on nykyisin melko kattavaa, käytännön kokemuksen, luottamuksen ja käyttäytymismallien puuttumista voidaan pitää esteenä sähköisten sopimusten tekemisen yleistymiselle ja kasvulle. Esteitä on pyritty poistamaan kehittämällä osapuolten tunnistamiseen ja sisällön varmistamiseen erilaisia menetelmiä, kuten esimerkiksi varmennettuja sähköisiä allekirjoituksia.

Sähköiset allekirjoitukset laajassa mielessä ovat olleet jo pitkään käytössä. Kertakäyttöiset TUPAS-pankkitunnisteet ovat Suomessa yleisin sähköisen allekirjoituksen muoto, vaikka ne eivät täytä lain vaatimuksia kehittyneen sähköisen allekirjoituksen osalta. Ongelmana yksinkertaisissa sähköissä allekirjoituksissa on niillä

tehtyjen oikeustoimen todennettavuuteen, muotomääräyksiin ja eheyteen liittyvät puutteet. Esimerkiksi muotomääräysten yhteensovittaminen on ongelmallista, jos perinteinen asiakirja menettää sähköisen tiedonsiirron yhteydessä alkuperäisyyttä osoittavaa ominaisuuttaan. Perinteisiä muotomääräyksiä sähköisessä toimintaympäristössä sovellettaessa voi syntyä ongelmia, jotka eivät ole käytännössä kovinkaan relevantteja, johtuen siitä että sähköisissä sopimuksissa harvemmin vaaditaan tiettyä muotoa.

Varmennettu julkisen avaimen tekniikalla tehty sähköinen allekirjoitus täyttää kaikki samat oikeudelliset vaatimukset kuin omakätinen allekirjoitus. Luotettavan julkisen avaimen tekniikkaa käyttävän osapuolen avulla toisilleen tuntemattomat osapuolet voivat luottaa toisiinsa sähköisessä ympäristössä. Näin voidaan lisätä turvallisuutta sopimuksenteossa avoimessa tietoverkossa, vaikka sopijapuolet eivät ole etukäteen sopineet tunnistamisen ja varmentamisen kysymyksistä.

Kehittyneet sähköiset allekirjoitukset ovat kuitenkin yleistyneet paljon hitaammin kuin vuosituhanteen vaihteessa oletettiin, ja markkinat ovat tällä hetkellä melko kehittymättömät. Suurimpina syinä sähköisten allekirjoitusten käyttöönottamisen hitaudelle voidaan pitää oikeusvarmuuden ja luottamuksen puutetta. Vaikka lainsäädännöllisesti sähköiset allekirjoitukset ovat hyvin yksityiskohtaisesti säänneltyjä, ei vielä ole kovinkaan kattavaa oikeuskäytäntöä, jonka perusteella voitaisiin arvioida erilaisten sähköisten allekirjoitusten tunnustamista käytännössä.[248]

Merkittävänä hidasteena sähköisten allekirjoitusten käytön yleistymisessä on ollut myös kuluttajien ja elinkeinonharjoittajien luottamuksen puute verkkoliiketoimintaan. Oikeustoimien tekemistä ei koeta turvalliseksi, kun henkilökohtainen kontakti toiseen osapuoleen puuttuu.

Kysymykseen siitä, miksi varmennetun sähköisen allekirjoituksen käyttö verkossa tapahtuvassa kaupankäynnissä ei ole kasvanut nykyistä nopeammin, ei liene yksiselitteistä vastausta, vaan ongelmia tuntuu olevan lukuisia.

---

[248] KOM 2006/120/EY s. 5.

Usein esiin nostettu ongelma, joka saattaa hidastaa kehittyneiden tai varmennettujen sähköisten allekirjoitusten käyttöönottoa Euroopassa, on julkisen avaimen tekniikan monimutkaisuus. Myös varmennetun sähköisen allekirjoituksen tekemiseen tarvittavat tekniset välineet ja niihin liittyvät kustannukset ovat ongelmatekijä. Kuluttajat eivät halua investoida korttiin ja lukulaitteisiin rahaa, eivätkä teknistä tietämystä vaativat laitevaatimukset ja epäselvät sekä monimutkaiset käyttöliittymät lisää intoa sähköisen allekirjoituksen käyttöönottoon. Ohjeistukseen laitteista ja ohjelmistoista tulisi kiinnittää lisää huomiota.

EU-säännösten puute koskien varmennepalvelun tarjoajan edellytystä tarjota sähköisen allekirjoituksen todentamispalveluja loppukäyttäjälle ja varmennepalvelujen keskinäistä tunnustamista on myös merkittävä. Monissa nykyisissä sovelluksissa palveluntarjoaja on haluton myöntämään vastuusyistä johtuen asiakkailleen oikeutta käyttää todentamismenetelmäänsä muissa palveluissa. Palveluntarjoajilla ei ole paljoakaan kannustimia kehittää moniin sovelluksiin sopivia sähköisiä allekirjoituksia, vaan ne tarjoavat mieluummin vain omiin palveluihinsa soveltuvia ratkaisuja, tästä esimerkkinä pankkialan kehittämät ratkaisut. Todennäköisesti tästä syystä johtuen markkinoilla käytetään edelleen erilaisia kertakäyttösalasanoja.[249]

Myös sähköisesti allekirjoitettujen asiakirjojen arkistointia pidetään liian monimutkaisena ja epävarmana toteuttaa. Arkistojen säilyttämiseen liittyviä kustannuksia kartetaan. Lakisääteinen velvollisuus säilyttää asiakirjat jopa yli 30 vuotta edellyttää kallista ja työlästä tekniikka ja organisointia, jotta asiakirjojen luotettavuus ja aitous voitaisiin varmistaa näin pitkään.

Suomen pienikokoiset markkinat eivät edesauta laatuvarmenteita tarjoavien tahojen markkinoille tuloa. Suomessa sähköisiä allekirjoituksia koskevan lain kriteerit täyttäviä laatuvarmenteita tarjoaa ainoastaan väestörekisterikeskus. Varmenteiden myöntäminen Suomessa on pikemminkin peruspalvelun tuottamista kuin tuottoisaa liiketointa.[250]

---

[249] KOM 2006/120/EY s. 7.
[250] Järvinen 2003 s. 171–172.

Toisena syynä tarjonnan vähäisyyteen voidaan pitää sitä, että Suomessa laatuvarmenteen myöntäjä voi joutua vahingonkorvausvelvolliseksi, esimerkiksi varmenteen mitätöimispyynnön käsittelyn viivästymisen vuoksi. Riski vahingonkorvausvelvolliseksi joutumisesta pienentää entisestään kiinnostuneiden tahojen määrää, mikä yhä vääristää kilpailutilannetta vähentäen varmenteiden käyttöönottoa.

Väestörekisterikeskuksen myöntämää HST-korttia käyttää tällä hetkellä vain murto-osa suomalaisista. HST-korttia hyödyntävien palveluiden määrä on vielä kovin vähäinen ja palvelut ovat lähinnä valtiohallinnon palveluja. HST-kortin uskottavuusongelmasta kertoo se, että henkilökohtaisissa pankkipalveluissa käytetään edelleen lähes pelkästään TUPAS-pankkitunnisteita.

Tulevaisuudessa varmennettujen sähköisten allekirjoitusten tai vastaavien käyttö tulee todennäköisesti kuitenkin yleistymään. On vaikea sanoa, kehittyykö HST-kortista koskaan jokapäiväistä sähköistä allekirjoittamisvälinettä, mutta edellytykset ovat olemassa. HST-kortin menestymisen kannalta käyttäjiä ja palveluja tulisi saada huomattavasti lisää. Ongelmana lienee, että ei toista ilman edellistä. HST-kortin jakaminen ilmaiseksi, kuten kansallisessa tietoyhteiskuntastrategia 2007 – 2015:ssa ehdotettiin, voisi olla kansalaisille tarvittava insentiivi. Kiinnostusta lisäisi myös jos HST-kortti kävisi myös ulkomailla[251] sähköisestä allekirjoituksesta ja tunnisteesta, esimerkiksi jos koko EU:n alueella olisi yksi yhtenäinen kortti. EU:n komissiolla on jo pyrkimyksenä kiinnittää huomiota sähköisten allekirjoitusten toimivuuteen ja käyttöön maiden rajojen yli.[252]

Käyttäjämäärän sekä palveluiden ja sovellusten määrän kasvu voi lisätä tulevaisuudessa HST-kortin käyttöä merkittävästi, koska kansalaisilla on tarve luotettavalle todentamisenvälineelle. Varmenteiden leviäminen erilaisille älykorttialustoille, kuten esimerkiksi pankkikorteille ja matkapuhelinoperaattoreiden SIM-korteille tulee osaltaan laskemaan kynnystä sähköiseen asiointiin.

---

[251] Liikenne- ja viestintäministeriö 2005b s. 37. Suomen HST-kortti käy ainoastaan Itävallassa sähköisenä tunnisteena.
[252] KOM 2006/120/EY s. 10-11.

Tietoyhteiskunnan palvelujen kehittämisen yhteydessä on myös hahmoteltu biometrisen laatuvarmenteen kehittämisestä. Esimerkiksi sormenjälkeen perustuva laatuvarmenne lisäisi älykorttipohjaisen sähköisen allekirjoituksen luotettavuutta ja tekisi siitä hyvin vaikean väärentää. Tulevaisuuden uhkakuvana tässäkin asiassa voidaan pitää biometriseen rekisteriin liittyviä riskejä henkilön anonymiteetille.

Lähteet

Kirjallisuus

Baum, Michael ja Perritt, Jr. Henry 1991. Electronic Contracting, Publishing and EDI LAW. Wiley Law Publications, New York.

Heikkilä, Juha ja Laine, Juha 2001. Elektroninen liiketoiminta. Laineen (toim.) teoksessa Verkkokauppaoikeus, ks. alla.

Hemmo, Mika 2003. Sopimusoikeus I, 2. uudistettu painos. Talentum, Helsinki.

Hoppu, Esko ja Hoppu, Kari 2007. Kauppa- ja varallisuusoikeuden pääpiirteet. WSOYpro, Helsinki.

Järvinen, Petteri 2003. Salausmenetelmät. Docendo, Jyväskylä.

Kivimäki, T.M ja Ylöstalo, Matti 1981. Suomen siviilioikeuden oppikirja. WSOY, Porvoo.

Laine, Juha 1998. Kuluttajansuojasta kansainvälisessä verkkokaupassa. LTT-tutkimus, Helsinki.

Laine, Juha 2001. Verkkokaupan sopimuksista. Laineen (toim.) teoksessa Verkkokauppaoikeus. WSOY, Porvoo.

Nurmela, Juha, Sirkiä, Timo ja Muttilainen,Vesa 2007. Suomalaiset tietoyhteiskunnassa 2006. Tilastokeskus, Helsinki.

Nurmi, Risto 1997. Elektroninen sopimus: elektronisen sopimusilmaisun sitovuusperusteista. Lakimiesliiton kustannus, Helsinki.

Rahnasto, Ilkka 2002. Internet-oikeuden perusteet. Kauppakaari, Helsinki.

Rinne, Timo 2002. Älykortit: Tekniikka, sovellusalueet ja käyttöönotto. Satku.fi, Helsinki.

Artikkelit

Dumortier, Jos ja Van den Eynde, Sofie (2002). Electronic Signatures and Trusted Archival Services. Saatavilla http://www.law.kuleuven.ac.be/icri/publications/172DLM2002.pdf?where=, vierailtu 23.2.2008.

Moilanen, Niko, Pellinen, Jari ja Romanainen, Lassi (2002). Suojatut tietoyhteydet. Seminaarityö. Saatavilla http://www.it.lut.fi/kurssit/01-02/010628000/semmat/SSL-tunnistus.pdf, 5.2.2008.

Männikkö, Päivi 2007. Sähköisen asioinnin tunnistuspalvelut hakevat vielä uomiaan – luottamus avainasemassa. Uusi kuluttajansuoja 1/2007, s.11-16.

Nimmer, Raymond 1996. Electronic Contracting: Legal Issues. The John Marshall Journal of Computer & Information law 14/1996, vuosikirja, s. 211-246.

Puurunen, Tapio 2005. Elektroninen kauppa haastaa oikeudelliset rakenteet. Lakimiesuutiset 5/2005, s. 14-15.

Railas, Lauri 2005. Sähköiset sopimukset kansainvälisessä kaupassa – UNCITRAL:in uusi yleissopimus. Defensor Legis 6/2005, s. 1268-1291.

Railas, Lauri 2006. Sähköisen tunnistautumisen haasteet Suomessa ja Euroopassa. Esitys HELSINKI ICT WEEK 2006 – seminaarissa. Saatavilla http://www.tieke.fi/mp/db/material_folder/x/IMG/19522:19515/file/SahkoisentunnistamisenhaasteetRailasAsianajotoimistoKrogerusOy.pdf, 1.2.2008.

Lainsäädäntö

Direktiivi kuluttajansuojasta etäsopimuksissa 97/7/EY
Direktiivi teknisiä standardeja ja määräyksiä ja tietoyhteiskunnan palveluja koskevia määräyksiä koskevien tietojen toimittamisessa noudatettavasta menettelystä 98/48/EY
Direktiivi sähköisiä allekirjoituksia koskevista yhteisön puitteista 99/93/EY
Direktiivi sähköisestä kaupankäynnistä 2000/31/EY

Kuluttajansuojalaki 20.1.1978/38
Laki sähköisistä allekirjoituksista 24.1.2003/14
Laki sähköisestä asioinnista viranomaistoiminnassa 24.1.2003/13
Laki tietoyhteiskunnan palvelujen tarjoamisesta 5.6.2002/458
Laki varallisuusoikeudellisista oikeustoimista 13.6.1929/228

Hallituksen esitykset

HE 79/2000	Hallituksen esitys Eduskunnalle laeiksi kuluttajansuojalain ja sopimattomasta menettelystä elinkeinotoiminnassa annetun lain 2 §:n muuttamisesta
HE 194/2001	Hallituksen esitys Eduskunnalle laiksi tietoyhteiskunnan palvelujen tarjoamisesta
HE 197/2001	Hallituksen esitys Eduskunnalle laiksi sähköisistä allekirjoituksista

Muut

KOM 1990:20	Oikeustoimilakitoimikunnan mietintö
KOM 1998/586/EY	Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi sähköistä kaupankäyntiä sisämarkkinoilla koskevista tietyistä oikeudellisista näkökohdista (lopullinen)
KOM 2003/567/EY	Sähköisen hallinnon merkitys Euroopassa

KOM 2006/120/EY Euroopan yhteisöjen komission kertomus Euroopan parlamentille ja neuvostolle sähköisiä allekirjoituksia koskevista puitteista direktiivin toteuttamisesta (1999/93/EY)

SEK/2000/0386 Komission tiedonanto neuvoston yhteisestä kannasta ehdotukseen direktiiviksi sähköisestä kaupankäynnistä (lopullinen)

Ohjeet, määräykset ja virallisselvitykset

HST työryhmä 2003. HST arkkitehtuurit ja liiketoimintamallit. Määrittely, versio 1.0. Helsinki.

Kuluttajatutkimuskeskus 2007. Tunnisteilla turvallisuutta – tutkimus sähköisten tunnisteiden käytöstä. Julkaisu 6/2007. Helsinki. Saatavilla http://www.kuluttajatutkimuskeskus.fi/files/5069/2007_06_julkaisu_tunnisteet.pdf, 2.3.2008.

Liikenne- ja viestintäministeriö 2003. Sähköisen tunnistamisen menetelmät ja niiden sääntelyn tarve. Julkaisu 44/2003. Helsinki.

Liikenne- ja viestintäministeriö 2005a. Turvalliset sähköisen allekirjoituksen luomisvälineet. Vaatimusten arviointi. Julkaisu 52/2005. Helsinki.

Liikenne- ja viestintäministeriö 2005b. Laki sähköisistä allekirjoituksista 14/2003 – vaikutusten arviointi. Julkaisu 53/2005. Helsinki.

Valtiovarainministeriö 2001. Tietojärjestelmien ajan määräytyminen ja aikaleimapalvelut hallinnon sähköisessä asioinnissa. Työryhmämuistio 5/2001.

Valtiovarainministeriö 2006. Tunnistaminen julkishallinnon verkkopalveluissa. Ohje 40/01/2006. Helsinki.

Viestintäministeriö 2003. Määräys laatuvarmenteita tarjoavien varmentajien ilmoitusvelvollisuudesta viestintävirastolle. Määräys 7/2003. Helsinki.

Valtioneuvoston päätös teknisiä määräyksiä koskevien tietojen toimittamisesta noudatettavasta menettelystä 802/1999.

Internet-lähteet

Australian IT 2007. More personal data lost in the uk. Saatavilla http://www.australianit.news.com.au/story/0,24897,22968521-15306,00.html, 5.3.2008.

BBC News 2007. UK's families put on fraud alert. Saatavilla http://news.bbc.co.uk/go/pr/fr/-/1/hi/uk_politics/7103566.stm, 5.3.2008.

Poliisi. Henkilökortit. Saatavilla www.poliisi.fi / luvat / henkilökortit / Henkilökortit, 04.02.2008.

The Times 2008. Personal data of 600,000 on lost laptop. Saatavilla http://www.timesonline.co.uk/tol/news/politics/article3213274.ece, 5.3.2008.

Tietoyhteiskunnan kehittämiskeskus ry. Yritysten välisen sähköisen kaupan oikeudellisia kysymyksiä. Saatavilla www.tieke.fi / Julkaisut / Oppaat yrityksille / Sähköisen kaupankäynnin aapinen / sähköisen kaupankäynnin oikeudelliset kysymykset / Yritysten välisen sähköisen kaupan oikeudellisia kysymyksiä, 11.2.2008.

Työ- ja elinkeinoministeriö. EU:n ilmoitusmenettely. Saatavilla www.tem.fi / Kuluttajat ja markkinat / Tavaroiden ja palveluiden vapaa liikkuvuus / EU:n ilmoitusmenettely, 26.02.2008.

Väestörekisterikeskus 2003. Väestörekisterikeskus julkaisee avoimen lähdekoodin sähköisten asiointipalvelujen rakentajille. Saatavilla http://www.vaestorekisterikeskus.fi/vrk/bulletin.nsf/vwSearchView/EA405E8936FF1155C2256D0A002BAF31, 2.3.2008.

Väestörekisterikeskus 2008. 01.01.2008 Joulukuun 2007 loppuun mennessä kansalaisvarmennetta oli myönnetty 169.400:lle henkilölle. Saatavilla www.sahkoinenhenkilokortti.fi / lisää tiedotteita / 01.01.2008 Joulukuun 2007 loppuun mennessä kansalaisvarmennetta oli myönnetty 169.400:lle henkilölle, 01.02.2008.

Väestörekisterikeskus 2008. @tu-klubi – uutiskanava sirullisesta henkilökortista ja asioinnista. Väestörekisterikeskus luotettava varmentaja Microsoft Windows –käyttöjärjestelmässä. Saatavilla www.etu-klubi.fi / Väestörekisterikeskus luotettava varmentaja Microsoft Windows –käyttöjärjestelmässä, 26.01.2008.

Liite 1: Direktiivin sähköisiä allekirjoituksia koskevista yhteisön puitteista liitteet I–IV

Direktiivin sähköisiä allekirjoituksia koskevista yhteisön puitteista liite I: Hyväksyttyjä varmenteita koskevat vaatimukset

Hyväksytyssä varmenteessa on oltava:

a) osoitus siitä, että varmenne on myönnetty hyväksyttynä varmenteena;

b) tiedot varmennepalvelujen tarjoajasta ja valtiosta, johon se on sijoittautunut;

c) allekirjoittajan nimi tai salanimi, jonka osalta on mainittava kyseessä olevan salanimi;

d) mahdollisuus lisätä allekirjoittajaan liittyvä asiaankuuluva erityismääre, riippuen varmenteen aiotusta käyttötarkoituksesta;

e) allekirjoituksen todentamiseen käytettävät tiedot, jotka vastaavat allekirjoittajan valvonnassa olevia allekirjoituksen
luomiseen käytettäviä tietoja;

f) tieto varmenteen voimassaoloajan alkamis- ja päättymisajankohdasta;

g) varmenteen tunnuskoodi;

h) varmenteen myöntävän varmennepalvelujen tarjoajan kehittynyt sähköinen allekirjoitus;

i) mahdolliset varmenteen käyttörajoitukset; ja

j) mahdolliset arvomääräiset rajoitukset toimille, joihin varmennetta voidaan käyttää.

Direktiivin sähköisiä allekirjoituksia koskevista yhteisön puitteista liite II: Hyväksyttyjä varmenteita myöntävien varmennepalvelujen tarjojia koskevat vaatimukset

Varmennepalvelujen tarjoajien on:

a) osoitettava varmennepalvelujen tarjoamisen edellyttämä luotettavuus;

b) varmistettava nopea ja varma hakemistopalvelu sekä luotettava ja viivytyksetön peruuttamismahdollisuus;

c) varmistettava, että varmenteen myöntämisen tai peruuttamisen päivämäärä ja aika voidaan määrittää tarkasti;

d) todennettava tarkoituksenmukaisin keinoin kansallisen lainsäädännön mukaisesti sen henkilön henkilöllisyys ja tarvittaessa
tietyt erityismääreet, jolle hyväksytty varmenne on myönnetty;

e) pidettävä palveluksessaan henkilökuntaa, jolla on tarjottujen palvelujen edellyttämä asiantuntemus, kokemus ja pätevyys
varsinkin johtotehtävissä toimivien osalta, sähköisten allekirjoitusten tekniikoihin liittyvä asiantuntemus ja
tarkoituksenmukaisten turvatoimien tuntemus; palvelujen tarjoajien on lisäksi noudatettava asianmukaisia ja tunnustettujen
standardien mukaisia hallinnollisia ja liikkeenjohdollisia menetelytapoja;

f) käytettävä luotettavia järjestelmiä ja tuotteita, jotka on suojattu muutoksilta ja joilla varmistetaan tuotteiden tukemien
prosessien turvallisuus niin tekniikan kuin salaamisen osalta;

g) toteutettava toimenpiteet varmenteiden väärentämisen ehkäisemiseksi ja, silloin kun varmennepalvelun tarjoaja luo
allekirjoituksen luomiseen käytettävät tiedot, taattava luottamuksellisuus kyseisiä tietoja luotaessa;

h) hallittava tämän direktiivin vaatimusten mukaisen toiminnan edellyttämiä varoja varsinkin vahinkovastuiden kattamiseksi,
esimerkiksi asianmukaisella vakuutuksella;

i) arkistoitava kaikki asiaankuuluvat hyväksyttyä varmennetta koskevat tiedot tarkoituksenmukaiseksi ajaksi erityisesti

voidakseen esittää varmentamista koskevia todisteita oikeudellisissa menettelyissä. Tällaisia arkistoja voidaan ylläpitää
sähköisessä muodossa;
j) oltava tallentamatta tai jäljentämättä varmennepalvelujen tarjoajalta salausavaimen hallintapalveluja saaneen henkilön
allekirjoituksen luomiseen käytettäviä tietoja;
k) ennen ryhtymistä sopimussuhteeseen sähköiselle allekirjoitukselleen varmennusta hakevan henkilön kanssa ilmoitettava
kyseiselle henkilölle tiedon säilyttävää viestintämuotoa käyttäen varmenteen käytön tarkoista ehdoista ja edellytyksistä,
mukaan lukien sen käyttörajoitukset, vapaaehtoisuuteen perustuvan akkreditointijärjestelmän olemassaolosta sekä
valitus- ja riitojenratkaisumenettelyistä. Nämä tiedot, jotka voidaan toimittaa sähköisesti, on annettava kirjallisesti ja
selvästi ymmärrettävällä kielellä. Näiden tietojen olennaisten kohtien on lisäksi pyynnöstä oltava varmenteeseen
tukeutuvien kolmansien osapuolien saatavilla;
l) käytettävä luotettavia järjestelmiä varmenteiden tallentamiseen todennettavassa muodossa siten, että
— ainoastaan valtuutetut henkilöt voivat syöttää tietoja ja tehdä niihin muutoksia,
— tietojen aitous voidaan tarkistaa,
— yleisöllä on oikeus tehdä varmenteita koskevia hakuja vain silloin, kun varmenteen haltijalta on saatu lupa, ja
— että näitä turvallisuusvaatimuksia vaarantavat tekniset muutokset ovat operaattorin nähtävissä.

Direktiivin sähköisiä allekirjoituksia koskevista yhteisön puitteista liite III: Turvallisia allekirjoituksen luomismenetelmiä koskevat vaatimukset

1. Turvallisilla allekirjoituksen luomismenetelmillä on tarkoituksenmukaista tekniikkaa ja menettelytapoja käyttäen
varmistettava ainakin, että
a) allekirjoituksen luomiseen käytettäviä tietoja voi käytännössä käyttää vain kerran ja että niiden luottamuksellisuus
voidaan kohtuudella varmistaa;
b) allekirjoituksen luomiseen käytettäviä tietoja ei voi kohtuullisella varmuudella johtaa ja että allekirjoitus on suojattu
kulloinkin käytössä olevaa tekniikkaa käyttäen suoritettavalta väärentämiseltä;
c) laillinen allekirjoittaja voi luotettavasti suojata allekirjoituksen luomiseen käytettävät tiedot muiden käytöltä.
2. Turvalliset allekirjoituksen luomismenetelmät eivät saa muuttaa allekirjoitettavia tietoja eivätkä estää niiden esittämistä allekirjoittajalle ennen allekirjoittamismenettelyä.

Direktiivin sähköisiä allekirjoituksia koskevista yhteisön puitteista liite IV: Turvallista allekirjoitusten todentamista koskevat suositukset

Allekirjoituksen todentamismenettelyn aikana olisi kohtuullisella varmuudella varmistettava, että:

a) allekirjoituksen todentamiseen käytettävät tiedot vastaavat todentajalle näkyvissä olevia tietoja;

b) allekirjoitus todennetaan luotettavasti ja että todentamisen tulos on asianmukaisesti nähtävissä;

c) todentaja voi tarvittaessa luotettavasti todeta allekirjoitettujen tietojen sisällön;

d) allekirjoituksen todentamishetkellä vaaditun varmenteen aitous ja pätevyys voidaan luotettavasti todentaa;

e) todentamisen tulos ja allekirjoittajan henkilöllisyys ovat asianmukaisesti nähtävissä;

f) salanimen käyttö on osoitettu selvästi; ja

g) kaikki turvallisuuteen liittyvät muutokset ovat havaittavissa.